Image Encryption using (k, n) Secret Sharing Scheme using Lagrange Polynomial

GVSS Jayanth Anish

Department of Information Technology, VIT University

Abstract: ***In this project a new (k, n) secret sharing scheme for image encryption is used. The proposed method encrypts the secret image into two images which are of the same size as that of the original image, in which one image is the public image (called the encrypted image) and another image is to be shared among n participants employing a new secret sharing method supported by the Shamir's secret sharing. In the new secret sharing scheme, k (or more) shares secretly held by the participants could reconstruct the shared image, where the size of each share is 2 (logkm)/m2 of that of the shared m*m image. Then the secret image can be recovered by using the encrypted image and the shared image without any loss. Further, the size of the shares can become smaller by partitioning the secret image into many smaller blocks and encrypting all these block images into a public encrypted image as the same size of the secret image. Compared with the previously known image encryption techniques based on the secret sharing, the size of the shares in our technique is smaller with the same size as that of original image.***

Keywords: Image Encryption, Lagrange Polynomial

1. Introduction

A (k, n) secret sharing scheme is a cryptographic primitive used to distribute a secret s to n participants in such a way that a set of k (or more) participants can recover the secret s and a set of k −1 (or fewer) participants cannot recover the secret s. A piece of shadow held by participants is called a share. Here in our project, we propose a secret sharing scheme for black & white (b & w), gray-level and color images based on Shamir secret sharing. In this scheme, the share obtained for each participant has a far smaller size than the secret image and the recovered image is exactly the same as the original one without any loss. Thus, the scheme is very fit to be applied in the wireless network and the IC Card system for image encryption.

Moreover, secret sharing schemes satisfying the additional property that unqualified subsets can gain absolutely no information about the secret are called perfect schemes.

Secret sharing schemes are very useful in some application fields, such as access control, opening a bank vault, opening a safety deposit box, or even launching missiles.

2. Literature Survey

1) Secret Sharing Scheme for Image Encryption Using new Transformation Matrix

This paper Introduces an image encryption and decryption process by using a new transformation matrix. The image is divided into zones. The zones are constructed from blocks of size 3 x 3 using secret keys. All the zones are combined together to form a new transformation matrix and are used for encryption purposes. The sender will send the secret in the form of polynomial's function value for their ID value.

The receiver will reconstruct the secret from the polynomial's function value. Then we can form the transformation matrix and decrypt it to get the original image. The comparison of the proposed method with the Cross Chaotic map image encryption method reveals that the proposed method is higher in security and superior in encryption quality and also the share to be sent is smaller.

2) A (t, n) Secret Sharing Scheme for Image Encryption

In This paper a new (t, n) secret sharing scheme for image encryption is proposed. The proposed method will encrypt a secret image into two images which are of same size of the original image, which one is the public image (called the encrypted image) and another image is to be shared among n participants using a new secret sharing method based on the Shamir's secret sharing. In the new secret sharing scheme, t (or more) shares secretly held by the participants could reconstruct the shared image, where the size of each share is 2 (log m) t 2 / m of that of the shared m m× image. Then the secret image could be recovered from the encrypted image and the shared image through simple XOR operations without any loss. Furthermore, the shares size can become smaller by partitioning the secret image into many smaller blocks and encrypting all these block images into a public encrypted image as the same size of the secret image. Comparing with the already known image encryption schemes based on the secret sharing, the size of the shares in our scheme is smaller with the same size as that of original image.

3) Polynomial Substitution based Image Encryption using Shamir Scheme

In this paper an efficient (□, □) secret sharing is proposed for encryption of images based on polynomial substitution with Shamir secret sharing. The proposed technique enciphers the secret image as two different images: one is made public which is the enciphered image and an additional other one is secret that can be shared among the □ members. In the proposed method, □ − shares are implemented by □−participants. The pixel values of the secret image are treated as the coefficient in the polynomial equation. The reconstruction of the shares is done by the □ −participants and the probability of recovering the whole image is (1256) m without any errors. It reveals that the implemented scheme is highly secure from attacks. By solving the polynomial equations using recovered t −values the secret image can be recovered. A security analysis is also performed for the proposed method to show its efficiency.

4) Creation of pseudo-random sequences based on chaos for forming of wideband signal

The aim of the paper is the development of a technique for creating pseudo-random sequences based on chaos, as well as the analysis of the correlation characteristics of pseudo-random sequences formed on the basis of a chaotic signal. Chaotic signals are inherently pseudo-random, but they are generated by deterministic systems. All computer models of chaos are approximations of mathematical chaos. Any analysis of these sequences doesn't allow them to be reproduced and they can't be intercepted, so they have significant advantages when used for spreading the signal spectrum and creating a pseudo noise broadband signal. Sequence selection with an acceptable level of side lobes of the autocorrelation function is carried out by using the developed graphical interface method.

5) A New Technique for Image Encryption using RIJNDAEL Block Cipher Algorithms

This paper has proposed block cipher Rijndael algorithm and is used to encrypt and decrypt an image with a variable key length and variable block length. The authors in this paper focused on the quality measurement [s such as the speed, Encryption Ratio, Correlation Coefficient and Compression encryption has no effect on size of the JPEG image encryption with the existing bitmap image encryption. Since, the JPEG files are of compressed format and the compression friendliness is measured here. It is desirable that the size of encrypted data should not increase. The result ends with the comparison of performance parameters based on the type of files formats. Therefore for higher data encryption or multimedia encryption the compressed format can be applied and it will yield a higher encryption ratio.

6) Novel Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding

In this examination, they proposed a Grayscale picture encryption strategy dependent on RTSs and steganography. The proposed cryptosystem utilizes numerous RTSs and stage installing methods for the age of disarray in spatial and recurrence areas of mystery pictures. Fluffy methodology is utilized for the determination of RTSs. Investigations and correlation indicated that the proposed security framework is safer when contrasted with a few of the notable cryptosystems dependent on single S-box and mix of S-box and steganography. In future, the recently created calculation can be utilized for the encryption of shading picture and information concealing reason with certain changes.

7) Enhancing the Security in Cryptosystems Based on Magic Rectangle

Another encoding plan dependent on MR rather than existing ASCII based encoding plan has been thought of and the numerals associated with MR are utilized for encryption in RSA and ElGamal open key cryptosystems. The numerals are not handily followed by the busybody in light of the fact that the enchantment total, MRS and MRT utilized in producing the MR are just known to the sender what's more, the collector. Moreover, for a similar enchantment whole various MRs are created by exchanging columns or segments which will create various numerals at the same position without fail. This causes an extra layer of security for any cryptosystems before performing encryption and unscrambling. Further, to speed up cryptographic activities parallelism is utilized in this paper which depends on Maui scheduler in recreated condition with various processors.

8) An image encryption and decryption using AES algorithm

In this paper, Image Encryption and Decryption utilizing the AES calculation are actualized to make sure about the picture information from unapproved get to. Fruitful usage of symmetric key AES calculation is extraordinary compared to other encryption and decoding guidelines accessible in the market. With the assistance of MATLAB coding execution of an AES calculation is integrated and reenacted for Image Encryption and Decryption. The first pictures can likewise be totally reproduced with no contortion. It has demonstrated that the calculations have incredibly huge security key space and can withstand most normal assaults, for example, the animal power assault, figure assaults, and plaintext assaults.

9) Encryption On Grayscale Image For Digital Image Confidentiality Using Shamir Secret Sharing Scheme

In this study, the Secret Sharing Method was used by employing the Shamir Threshold Scheme Algorithm on grayscale digital images with the size of 256x256 pixel obtaining 128x128 pixels of shared image with threshold values (4, 8). The resulting number of shared images was 8 parts and the recovery process can be carried out by at least using 4 shares of the 8 parts. The result of this encryption on grayscale image is capable of producing a vague shared image (i.e., no perceptible information), therefore a message in the form of digital image can be kept confidential and secure.

10) Image Encryption Using Separable Reversible Data Hiding Scheme

An epic distinguishable reversible information concealing plan is executed for picture encryption. An info picture is encoded by the substance proprietor utilizing an encryption key. Information concealing key packs the least huge pieces of the encoded picture to make space to insert information. Haar wavelet lossy pressure procedure can't recover the picture proficiently contrasted with RLC lossless pressure method for quicker transmission. Picture encryption key is utilized to recover the picture and information concealing key for information extraction.

Picture encryption and information concealing keys can be utilized for concurrent extraction of the first substance by abusing the spatial relationship in a normal picture. Recreation results gotten are like the common substance.

Equipment execution for encryption and decoding of 32 x 32 pictures is actualized.

11) Non-expanded Visual Cryptography Scheme with Authentication

This paper combines the non-expanded scheme with the extra ability of hiding confidential data to prevent the detection of information. In the proposed scheme, the secret image is divided into four regions, and share blocks are subsequently generated by using the block encoding method with non-expansion ability. A certain sequence of original regions must be followed when generating region shares. Finally, the first share image is reversed and stacked with the other share image. The extra confidential data can be revealed, and it prevents the detection of information.

12) Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images

This paper proposed an encryption scheme with consisting of a new additive homomorphism based on Elliptic Curve ElGamal (EC-ElGamal) for sharing secret images over unsecured channels. The proposed scheme enables shorter keys and better performance than schemes based on RSA or ElGamal. It has a lower computation overhead in image decryption compared with the method that uses other additively homomorphic properties in EC-ElGamal. Elliptic curve parameters are selected to resist the Pohlig- Hellman, Pollard’s-rho, and Isomorphism attacks. Experimental results and analysis shows that the proposed method showed superior performance to RSA and ElGamal.

13) New Cryptography Algorithm withFuzzy Logic for Effective Data Communication

In this paper, people forget to care about security when the data communication gets the importance of privacy most of the time. There the data theft takes place effortlessly. Many methodologies have been devised for making effective communication either over the internet or intranet. However, the hackers enrich themselves more than the new technologies whenever they are launched. As need arises to cultivate the security key generation while secure data communication has to been assured, we propose a new cryptography algorithm along with the fuzzy logic through this paper that materializes the secure communication possible. Firstly, we observed the flaw that causes hacking effortlessly by the intruder during the data transmission over the network. Then the evaluation part could be done with the same context without losing data because of this proposed algorithm. The algorithm concentrates on image and text data encryption by using fuzzy logic and on secured sharing theme which provides highly authenticated data transferring. The existing security algorithms had a nod in many ways only for the secure data transmission rather than the complexity in which they have when needed to be executed.

Hence the aspirants who want to have the communication have to spend more time than the actual. Obviously the precious algorithms should have less processing time and are highly secure in nature. It keeps it as a main aspect the New Cryptography algorithm with fuzzy logic is proposed and has low process time and high security logics using various keys for encryption and decryption. The results which produced by this proposed algorithm have been compared with existing algorithms and finally could arrive at the conclusion that the proposed is highly effective in security aspects and needs a minimum amount of time to be executed.

14) Chaotic Genetic Encryption Technique

In this technique, binarize any digital datatype. The main encryption stages of Chaotic-GET are chaotic map functions, fuzzy logic and genetic operations. Mathematical operations and rotation are also included that increase encryption quality. Images are used for testing propose. For testing C-GET, digital images are used because they become an important resource of communication. The original and reconstructed data are identical. Experimental results show that C-GET technique has multilayer protection stages against various attacks and a powerful security based on the multi-stages, multiple parameters, fuzzy logic and genetic operations. The Data that is Decrypted is nearly randomness and has negligible correlation with secret data.

15) Overview on Selective Encryption of Image and Video: Challenges and Perspectives

In this paper it is discussed that traditional image and video content protection schemes, called fully layered, the whole content is first compressed. After that, the compressed bit stream is entirely encrypted using a standard cipher (DES, AES, IDEA, etc.). The specific characteristics of this kind of data (high-transmission rate with limited bandwidth) make standard encryption algorithms inadequate.

In addition to previous another limitation of fully layered systems consists of altering the whole bit stream syntax which may disable some codec functionalities. Selective encryption is now a new trend in image and video content protection. It does process of encrypting only a subset of the data. The Main aim of selective encryption is to reduce the amount of data in order to encrypt while preserving a sufficient level of security.

This computation saving is very much desirable especially in constrained communications (real-time networking, high-definition delivery, and mobile communications with limited computational power devices). In addition to this, selective encryption allows preserving some codec functionalities such as scalability. This proposal is intended to give an overview on selective encryption algorithms. The theoretical background of selective encryption, potential applications, challenges, and perspectives is presented. ’

3. Shamirs Secret Sharing

This algorithm mainly divides any secret that is to be encrypted into various unique parts.

Process is:

- If S is the secret that is to be encrypted
- It will be divided into N parts
- After that a number K chosen for decrypting purpose
- K chosen in a way that if shares are less than k we can’t able to find secret
- For reconstruction of secret can’t be done with (k-1) or less shares
- If K shares available then it will be reconstructed.

Mathematically Shamir's secret sharing explained via this example:

Suppose that our secret is 1234.

We wish to divide the secret into 6 parts, where any subset of 3 parts is sufficient to reconstruct the secret.

At random we obtain numbers: 166 and 94.

$(a_0 = 1234; a_1 = 166; a_2 = 94)$, where a_0 is secret

The polynomial to produce secret shares (points) is therefore:

$$f(x) = 1234 + 166x + 94x^2$$

We construct six points D0, D1, D2, D3, D4, D5

$$D_0 = (1, 1494); D_1 = (2, 1942); D_2 = (3, 2578);$$

$$D_3 = (4, 3402); D_4 = (5, 4414); D_5 = (6, 5614)$$

And these will be distributed to get our secret back
In order to reconstruct the secret back any 3 points will be enough.

$$(x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414)$$

We will take these 3 points for getting our secret back

Based on lagranges interpolation

$$\ell_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2(x) = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore, by formula

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$1942\left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}\right) + 3402\left(-\frac{1}{2}x^2 + \frac{7}{2}x - 5\right) + 4414\left(\frac{1}{3}x^2 - 2x + \frac{8}{3}\right)$$

$$1234 + 166x + 94x^2$$

Thus secret 1234 is got back

4. Methodology

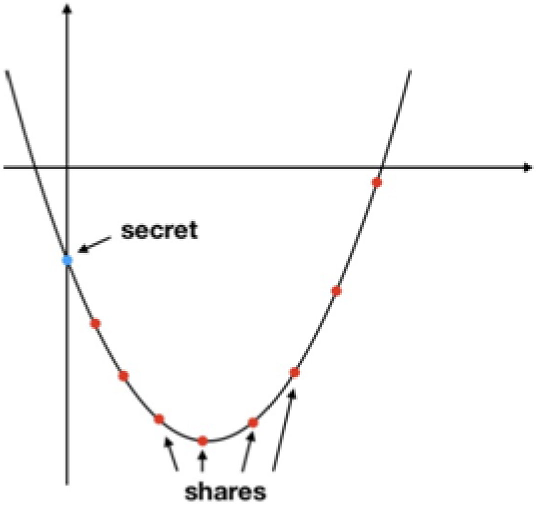
In this project, the Secret Sharing method put forward by Shamir is used. The aim is to distribute the secret data indicated by "S" to "n" people and to obtain the hidden secret by combining the "k" ones. Each person will have a share value. First of all, the function that will create the share values is determined.

f (x) = (S + ax + bx ^ 2 + cx ^ 3 +... + zx ^ (k-1)) mod p

Here, the definition range of values a, b, c, z is [0, p-1] and they are chosen randomly from this range. (While the "p" value is the prime 257 while storing the image) Then it is calculated on the 1st share, f (1) determines the value of the 1st share. Likewise, the value of the 2nd share is calculated with f (2), after the value of "n" denominators is calculated, random "k" grain is selected. These k denominators selected are used in Lagrange's interpolation to obtain hidden data.

Lagrange Interpolation:

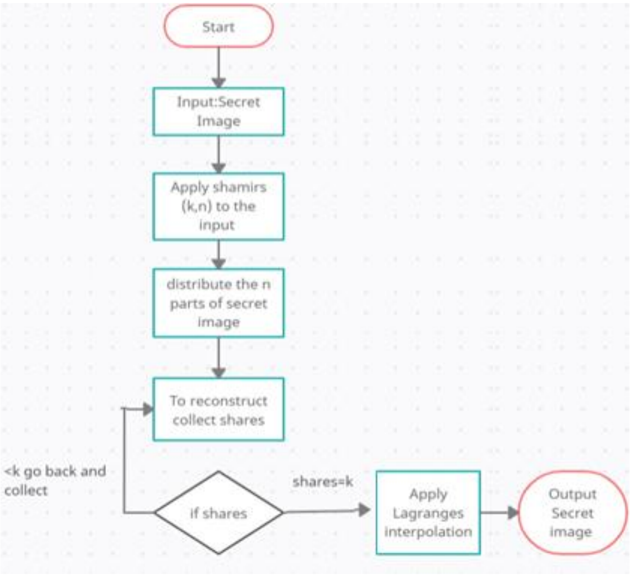
In Lagrange interpolation (n + 1), a function f (x) whose value (x, y) (x1, y1) (x2, y2) is known at the point (n + 1) is fitted with an L (x) polynomial whose values at these points are equal.



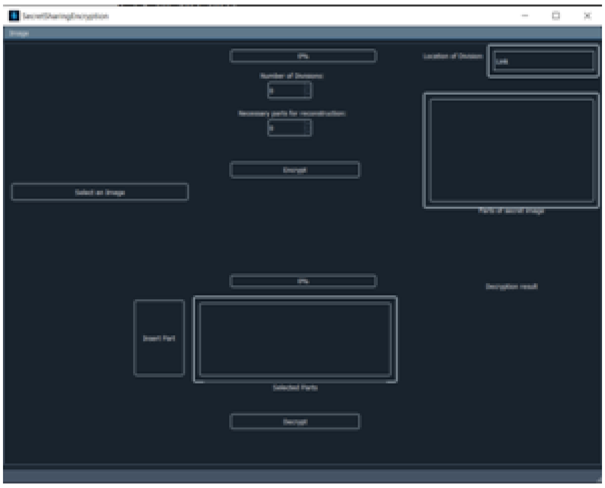
We convert the image into an array which contains the R, G and B values for each of the pixel.

Depending on the values of (k, n), we then generate n shares of images using the values we get by creating secret shares using the Shamir's scheme using lagrange's polynomial. These n shares can then be distributed through separate channels for security. When we need to get back the original image, we require at least k shares, and using the R, G, B values from these K shares, we use lagrange's interpolation to reconstruct the original image.

5. Flow Diagram

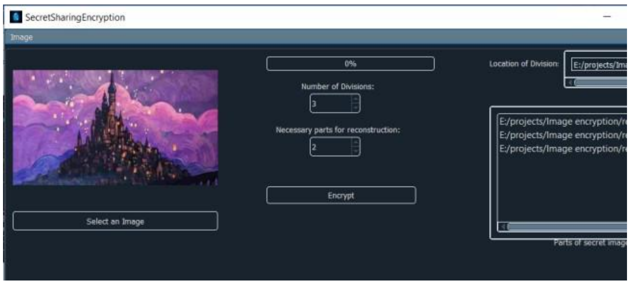

Start
Input:Secret Image
Apply shamirs (k,n) to the input
distribute the n parts of secret image
To reconstruct collect shares
<k go back and collect
if shares
shares=k
Apply Lagranges interpolation
Output Secret image

6. Results



Generating 3 encrypted images using (2,

3) Secret sharing scheme.



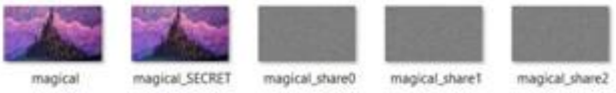
Location of Division: E:/projects/Ima

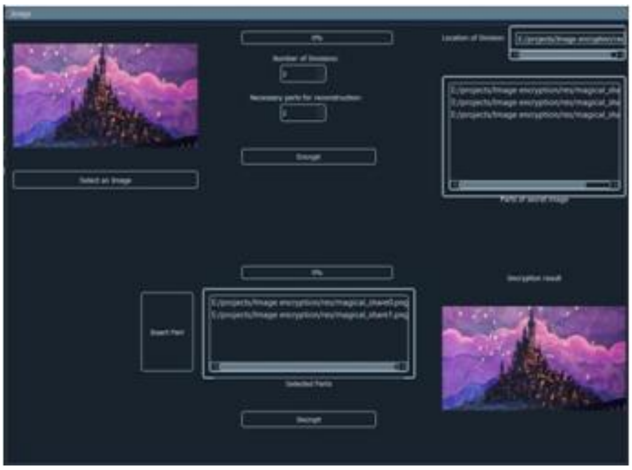
Number of Divisions: 3

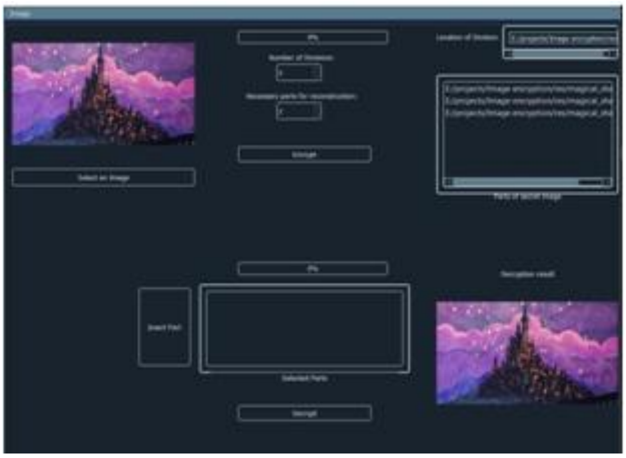
Necessary parts for reconstruction: 2

E:/projects/Image encryption/r
E:/projects/Image encryption/r
E:/projects/Image encryption/r

Input Image and corresponding 3 secret shares







7. Conclusion

For using a (k, n) scheme, we get ‘n’ encrypted shares, out of which ‘k’ shares are necessary for reconstruction of the image. With this technique, we can transfer confidential data securely with less chance of it being deciphered by any unauthorized person, due to sharing of secrets and avoiding any single point of attack. It can also provide redundancy, because only ‘k’ out of ‘n’ shares are required to reconstruct the image, therefore it can tolerate losses of some of the encrypted shares

References

[1] Kalai Selvi, and M. Mohamed Sathik, (2010), Secret Sharing Scheme for Image Encryption Using new Transformation Matrix, In International Conference on Advances in Information and Communication

[2] Technologies

[3] Runhua Shi, Hong Zhong, Liusheng Huang, and Yonglong Luo, (2008), A (t, n) secret sharing scheme for image encryption, In 2008 Congress on Image and Signal Processing

[4] R. Vidhya, and M. Brindha, (2019), Polynomial Substitution Based Image Encryption Using Shamir Scheme, International Journal of Computational Intelligence & IoT [4]Anatolii Semenko, Nikolai Kushnir, Nataliya Bokla,. Grigoriy Kosovan, (2017), CREATION OF Pseudo-random sequences based on chaos for forming of wideband signal, information and telecommunication sciences volume 8

[5] J. Mahalakshmi, K. Kuppusamy, (2012), A New Technique for Image Encryption using RIJNDAEL Block Cipher Algorithms, International Journal of Computer Applications

[6] Naveed Ahmed Azam, (2017), A NovelFuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding, Hindawi Security and Communication Networks

[7] Mani. K, Viswambari. M, (2017), Enhancing the Security in Cryptosystems Based on Magic Rectangle, I. J. Computer Network and Information Security

[8] Priya Deshmukh, (2016), An image encryption and decryption using AES algorithm, International Journal of Scientific & Engineering Research

[9] Rodiah, Dyah Anggraini, Fitrianingsih, Farizan Kazhimi, (2016), Encryption On Grayscale Image For

Digital Image Confidentiality Using Shamir Secret Sharing Scheme, Journal of Physics: Conference Series

[10] Smitha. M, Dr. V. E. Jayanthi, (2013), Image Encryption Using Separable Reversible Data Hiding Scheme, Institute of Electrical and Electronics Engineers (IEEE)

[11] Yi-Jing Huang, Jun-Dong Chang, (2013), Non-expanded Visual Cryptography Scheme with Authentication, Institute of Electrical and Electronics Engineers (IEEE)

[12] Li, Ahmed A. Abd El-Latif, Xiamu Niu, (2012), Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images, Signal Processing

[13] K. Ganesh Kumar, D. Arivazhagan, (2016), New Cryptography Algorithm with Fuzzy Logic for Effective Data Communication, Indian Journal of Science and Technology

[14] Hamdy M. Mousa, (2018), Chaotic Genetic-fuzzy Encryption Technique, International Journal of Computer Network and Information Security (IJCNIS)