A Survey on Cryptographic Algorithms Using Fractal Structures

Sneh Lata Aswal
Ph.D Scholar, U.T.U, Dehradun, Assistant Professor, Department of I.T, DIT University, Dehradun, Uttarakhand, India

Dr. Ashish Negi
Professor, Department of Computer Science and Application, G. B. Pant Engineering College, Pauri, Garhwal, Uttarakhand, India

Abstract:

Data security has become an important issue in recent times. Confidential data needs to be protected from unauthorized users. Various image encryption techniques have been proposed for the secure transmission of images to protect the authenticity, integrity and confidentiality of images. Fractal images can be used as a strong key for the encryption due to the random and chaotic nature of fractals. The infinite boundaries of fractals provide highly complex structure that leads to confusion and it becomes a tedious task for an unauthenticated user to crack the exact secret fractal key. In this paper, a review of various techniques used for image encryption using fractal geometry has been illustrated. All these techniques have their own advantages and disadvantages in terms of execution time, key generation time and Peak Signal to Noise Ratio.

Keywords- Cryptography, Encryption, Decryption, Fractal geometry, Image encryption, PSNR, Security, SSIM.

I. INTRODUCTION

The word fractal was coined by Mandelbrot in the 1970s. He dates the origin of 'Fractal Geometry' from 1975 but indicates that objects now considered as fractal existed long before that decade. Many naturally occurring objects, such as trees, coastlines or clouds, are now considered to have fractal properties; and much of the current interest in the topic stems from the attempts to simulate such natural phenomena using computer graphics[1]. Other more abstract forms of fractal objects were devised by artists and mathematicians, and again the availability of current techniques of computer graphics has given new insight into the structure of such objects.

The world as we know it is made up of objects which exist in integer dimensions, single dimensional points, one dimensional lines and curves, two dimension plane figures like circles and squares, and three dimensional solid objects such as spheres and cubes. However, many things in nature are described better with dimension being part of the way between two whole numbers [2]. While a straight line has a dimension of exactly one, a fractal curve will have a dimension between one and two, depending on how much space it takes up as it curves and twists. The more a fractal fills up a plane, the closer it approaches two dimensions. In the same manner of thinking, a wavy fractal scene will cover a dimension somewhere between two and three [3]. Hence, a fractal landscape which consists of a hill covered with tiny bumps would be closer to two dimensions, while a landscape composed of a rough surface with many average sized hills would be much closer to the third dimension.

For the most part, when the word fractal is mentioned, you immediately think of the stunning pictures you have seen that were called fractals. But just what exactly is a fractal? Basically, it is a rough geometric figure that has two properties: First, most magnified images of fractals are essentially indistinguishable from the unmagnified version [4]. This property of invariance under a change of scale if called self-similarity. Second, fractals have fractal dimensions, as were described above. The word fractal was invented by Benoit Mandelbrot, "I coined fractal from the Latin adjective fractus. The corresponding Latin verb frangere means to break to create irregular fragments. It is therefore sensible and how appropriate for our needs! - that, in addition to fragmented, fractus should also mean irregular, both meanings being preserved in fragment."

Graphically, fractals are images created out of the process of a mathematical exploration of the space in which they are plotted [5]. For this page, a computer screen will represent the space which is being explored. Each point in the area is tested in some way, usually an equation iterating for a given period of time. The equations used to test each point in the testing region are often extremely simple. Each particular point in the testing region is used as a starting point to test a given equation in a finite period of time. If the equation escapes, or becomes very large, within the period of time, it is colored white [6]. If doesn't escape, or stays within a given range throughout the time period, it is colored black. Hence, a fractal image is a graphical representation of the points which diverge, or go out of control, and the points which converge, or stay inside the set [7]. To make fractal images more elaborate and interesting, color is added to them. Rather than simply plotting a white point if it escapes, the point is assigned a color relative to how quickly it escaped. The images produced are very elaborate and possess non-Euclidean geometry. Fractals can also be produced by following a set of instructions such as remove the center third of a line segment [8].

The concept of fractals is used to create encryption methods in Visual cryptography. One of the main advantage of fractal objects is that they are infinite repetition of the same object so, when you introduce randomness in this process we get a pretty good cryptosystem. Fractal geometry is nature's geometry, so it is truly random but implementing fractal geometry in finite space with various constraints gives us a pseudo-fractal object [9,10].

There are lot of physical limitations which restricts fractal geometry to assume a truly random form. One of the successful implementation of fractal based encryption system is FITIN (Fractal Iteration of Information) which is understandably doesn’t use the fractal geometry to the fullest because of physical limitations. The fractal encryption which is achieved through this method is so far linear which makes it not so good for serious data encryption nevertheless it is step towards achieving the ultimate cryptosystem [11].

Before we go into details of FITIN, first let's understand a basic visual encryption method. In normal visual cryptography a image is encrypted by XORing the image with a key [12,13]. Key can be a small image with randomly selected pixel colors, now you keep XORing this key with the pixels of the actual image until you finish doing it to all the pixels in the image. Now what you get is a image which has unrelated pixel colors when compared to the actual image. This picture can be decrypted by XORing the encrypted picture with the same key which was used for encryption. This is a primitive example, lot of variable parameters can be used to make it even more harder to break[14,15].

II. LITERATURE SURVEY

Fractals were first used for text encryption by Jhansi et. al [16] where self-symmetric property of Sierpinsky fractal was used. The fractal curve was not used as a fractal key, only its geometry was used to encrypt the plaintext with the help of secret key (text). Sierpinsky triangle is a fractal that is generated by using a triangular initiator and connecting the mid-points of the three edges of the triangle to form four smaller triangles. On iterating this process on the smaller triangles a mathematical set which is known as Sierpinsky triangle is obtained [17].

The secret key bit was placed at the center while the plain text bit is placed in the surrounding triangles. Encryption algorithm used left-right circular shift operation and XOR-XNOR operations. The proposed algorithm is resistant to cipher text only attacks, known plaintext attack and chosen plaintext/cipher text attack and is on par with DES. This technique was used only for text data, hence there is a requirement for a robust technique for encryption of images. Using fractals for image encryption was first proposed in [18,19] where a selected square fractal key matrix was used as a fractal key. Matrix multiplication was used as the operation for encryption. The fractal encryption key is computed iteratively, changing fractal parameters as necessary, to obtain a full rank [11] fractal key matrix of size (NxN). The image data to be encrypted is buffered to form a two-dimensional matrix of size (JxN) or (NxJ) where J any be any positive integer including N. For a buffered data matrix of size (JxN), encryption uses matrix multiplication using the equation: $E= P*K$

where: P = the buffered data matrix (JxN);

K = the fractal key matrix (NxN); * indicates matrix multiplication;

E = the encrypted data matrix (NxJ).

After encryption, the encrypted matrix is sent to the receiver along with the fractal key parameters so that the same matrix can be generated at the receiver side and can be used as the decryption key [20,21]. The transmitted fractal key parameters must contain all the information necessary for the receiver to generate the fractal key, including but not limited to the fractal choice, any fractal initialization values, the fractal key matrix size (N), and the encrypted data matrix size (NxJ) or (JxN). The receiver performs the decryption using the available information using the equation:

$P=E*K^{-1}$

where: K^{-1}=the inverse fractal key matrix [22]. The proposed way of multiplication of the image matrix and the key matrix (the inverse key matrix) for encryption (decryption) is slow when it comes to big images. Also, it may require reformatting and post-processing at the receiver side. On applying the algorithm on a selected plain image using a Mandelbrot curve with certain parameters, we get a low PSNR value of 11.7241 for Red layer, 11.0069 for Green layer and 10.6269 for Blue layer. Another image encryption technique based on the modulo operation with fractal keys was proposed in [23,24]. The Mandelbrot set was generated using the bound set of S obtained from the recursive formula:

$$\forall \bar{x} \in C$$
$$S_{n+1}(\bar{x}) = \left[S_n(\bar{x}) \right]^a + b \times S_o(\bar{x})$$
$$a \in R, b \in C$$

The strength of the algorithm is determined by conducting the PSNR [25] test. The results show that the algorithm is strong enough to stand up to even the slightest changes in the key parameters and hence it is invulnerable to brute force attack [26,27] because the fractal key generation is time consuming. The value of the spacing δ must be small. The smaller the value of δ, the more secure encryption we achieve. This value cannot be extremely small nor can it be extremely large. The PSNR values as computed between the original image and the encrypted image by using a Mandelbrot curve created using specific parameters are 12.8619 for Red layer, 13.9165 for Green layer and 11.0339 for Blue layer. A technique based on matrix multiplication was proposed thereafter that involves compression of the image using fractal codes and then multiplying it with the selected fractal image matrix [15]. Both the matrices are first permuted which enhances the randomness in both the images [28,29].

Since fractal image has a very small memory footprint, memory requirement is quite low. Moreover, a slight difference in fractal parameters changes the fractal key to a great extent which makes the algorithm highly key sensitive. The key generation process is time consuming making it invulnerable to brute force attack. The algorithm results in a low PSNR value of 9.0470 for Red layer, 8.55 for Green layer and 7.58 for Blue layer. Mandelbrot set in a combination with Hilbert transformation has been used to enhance the randomness of the secret key in [30]. The Hilbert curve is a way of mapping the multidimensional space into a one-dimensional space. The Mandelbrot curve matrix is considered as the three layer matrix with RGB components. Each pixel $i(x,y)$ is mapped to a one-dimensional coordinate. An integer r is calculated that is the interval distance between one point to another while travelling the curve, to calculate the value of the pixel again. Each pixel in the image to be encrypted is labeled $O(x,y)$. $K(x,y)$ denotes the key and $T(x,y)$ denotes the encrypted image[31,32,33].

Mandelbrot fractal set in combination with Julia fractal set was used for a new key exchange protocol in [34]. The algorithm is based on the concepts of traditional Diffie-Hellman key exchange protocol [35]. The secret key is exchanged between the two users without any prior communication between them over an unsecure channel.

Much attention has been lately devoted to developing efficient and highly secure image encryption schemes. Image encryption algorithms are classified into three major categories [36,37]: (i) pixel position permutation based algorithms, in which a pixel is replaced by another pixel of the same image, (ii) value transformation based algorithms, in which a pixel is converted to another pixel value, and (iii) visual transformation based algorithms, in which another image is superimposed on another image such as using an image as a key or watermark-based encryption. Now, hybrid algorithms are most dominating. Different types of permutation or shuffling techniques have been successfully applied. Moreover, numerous frequency domain transforms have been considered. Furthermore, there is abundant literature on the use of chaotic maps as well as the use of fractals in image encryption [38].

For keystream generation, fractal geometry and chaotic maps have been extensively used in both cryptography and data hiding [39]. As for the use of chaotic function, Liu and Wang [40] used a piecewise linear chaotic map to generate a pseudorandom key stream sequence. Amin et al. [41] used a chaotic block cipher scheme to encrypt a block of bits rather than a block of pixels using cryptographic primitive operations and a nonlinear transformation function. Wang et al. in [42] encrypted images using Baker map and several one-dimensional chaotic maps. Wang et al. [43] encrypted plaintext by alternating between stream ciphering and block ciphering based on a pseudorandom number generated based on a chaotic map. On the other hand, Huang [44] used a nonlinear chaotic Chebyshev function to generate a keystream, in addition to multiple pixel permutations. In [45], Wang and Luan proposed a novel image encryption scheme based on reversible cellular automata combined with chaos.

As for the use of fractal images, the Mandelbulb set has been used in [46]. The fractal image and the fractal-compressed source image are transformed to square matrices and matrix operations are applied in encryption and decryption. The Mandelbrot set is utilized in [47] along with the Hilbert transformation to generate a random encryption key. Moreover, Abd-El-Hafiz et al. [47] introduced a novel image encryption system based on diffusion and confusion processes in which the image information is hidden inside the complex details of multiple fractal images.

The FFCT was first defined in [48] and corresponds to a finite field version of the discrete cosine transform (DCT). It exhibits interesting properties which are valuable for cryptographic purposes. In [27], a simple method for uniformizing histograms of greyscale digital images was introduced based on 8-point FFCT without any encryption mechanism. Then, a method for histogram uniformization of greyscale images integrated with a full encryption mechanism was developed in [27]. In [28], an improvement had been proposed to allow the color channels to be processed jointly by means of a single transformation round by using a 32-point FFCT over the to transform blocks of the image.

Nadia M. G and Saidi A.L in this paper a new image encoding system utilizing fractal theoriesis proposed. This approach exploits the main feature of fractals generated by IFS techniques. Two levels of encryption and decryption methods performed to enhance the security of the system. Theencrypted date represents the attractor generated by the IFStransformation, Collage theorem is usedto find the IFS for decrypting data. The proposed method gives the possibility to hide maximumamount of data in an image that represent the attractor of the IFS without degrading its quality. Alsoto make the hidden data robust enough to withstand known cryptographic attacks and imageprocessing techniques which do not change the appearance of image. The security level is highbecause the jointly coded images cannot be correctly reconstructed without all the requiredinformation.

Kaur G and Kaur M reported that Image compression is a method through which we canreduce the storage space of images, videos which will helpful to increase storage and transmissionprocess's performance, Images are compressed using lossy and Lossless compression schemes. Inthis paper Fractal image compression is discussed.Fractal image compression is a lossy compressionmethod for digital images, based on fractals. The method is best suited for textures and naturalimages, relying on the fact that parts of an image often resemble other parts of the same image.Fractal Encoding involves partitioning the images into Range Blocks and Domain. Blocks and eachRange Block is mapped onto the Domain Blocks by using contractive transforms called the Affine Transforms. The Fractal encoding technique takes a longer encoding time and less decoding time.

We are going to analyze soft computing techniques for fractal image compression.

Vanitha S.M and Kuppusamy K present a survey of the Fractal image compression. Fractalencoding is a mathematical process used to encode bitmaps containing a real-world image as a set ofmathematical data that describes the fractal properties of the image. A fractal is a structure that ismade up of similar forms and patterns that occur in many different sizes. The term fractal was firstused by Benoit Mandelbrot to describe repeating patterns that he observed occurring in manydifferent structures. In this context, the survey summarizes the major fractal imagecompression methods spanning across different fractal image compression techniques and comparedifferent fractal image compression techniques are distinct from each other. Further, the paper review that still research possibilities exist in this field to explore efficient fractal image compression [30].

Shaifali Agarwal,(2017) [49] summarizes the various recent image encryption techniques in which fractal key is used to encrypt/decrypt followed by substitution, scrambling and diffusion techniques to provide strong cryptosystem. The algorithms covered both private key encryption as well as public key encryption technique in the paper. The analyzed algorithms include a set of fractal function such as Mandelbrot set, Julia set, Hilbert curve, 3D fractal, multi-fractal, IFS and chaotic function to generate a complex key used in the encryption process. Corresponding performance of each algorithm is analyzed by PSNR test, key space, sensitivity analysis and correlation coefficient value between the adjacent pixels of both images (Original image and encrypted image) which shows significant improvement in performance over the traditional encryption methods.

III. CONCLUSION

Various techniques involving fractal geometry for image encryption are studied. All these techniques have their own advantages and disadvantages. The use of fractals enhances the perplexity of the encrypted image but at the same time it may prove to be complicated to the user itself. Fractal generation process is time consuming which is a disadvantage to the user as the whole encryption process will become time consuming, but on the other hand it is advantageous because cryptanalytic attacks such as brute force attack can be avoided due to the same. This is so because it would be a very tedious task for the attacker to guess the secret key since the Mandelbrot geometry is highly sensitive to a minute change in its parameters. The techniques can be classified based on PSNR values that define the Peak Signal to Noise Ratio between the original plain image and the encrypted image. The Mean Square Error (MSE) must be maximum between the original image and the encrypted image and hence the PSNR must be low because PSNR is inversely dependent on the MSE. Another metric to judge the image encryption techniques can be Structural Similarity (SSIM) Index [19]. SSIM is a full reference metric to measure the similarity between two images based on image quality. It considers the idea that the image pixels are strongly inter-dependent on each other when they are spatially close. SSIM does not estimate perceived errors; rather it is based on perceived change in structural information. While PSNR depends on the Mean Square Error only, SSIM takes into account variance and covariance between the two windows that are compared. Hence, SSIM proves to be consistent with human eye perception and provides more accurate results.

REFERENCES

[1] Diffie W., Hellman M., 1976 “New Directions in Cryptography”, IEEE Transactions on InformationTheory, 22(6): 644-654 doi-10.1109/TIT, 1055638.

[2] Rivest R. L., Shamir A. and Adleman L., 1978“A method for obtaining digital signatures and publickey cryptosystems”, Communication of the ACM, 21: pp 120-126.

[3] Mandelbrot B. B. “The Fractal Geometry of Nature”, W. H. Freeman, New York, 1983.

[4] Barnsley M. “Fractals everywhere”, Academic Press Professional, Inc., San Diego, CA, 1988.

[5] Pickover C. “Computers, Pattern, Chaos, and Beauty”, St. Martin’s Press, NewYork, 1990.

[6] W. S. Maki, Simple Geometric Fractals, Behavior Research Methods, Instruments and Computers, Psychonomic Society, Inc. 23(2), pp. 160-165, 1991.

[7] Devaney R. L., 1992 “A First Course in Chaotic Dynamical Systems: Theory and Experiment”,Addison-Wesley, MR1202237 Zbl 0768.58001.

[8] Crownover, R. M., “Introduction to Fractals and Chaos”, Jones &Barlett Publishers, 1995.

[9] Stallings W., 1999 “Cryptography and Network Security: Principles and Practice”. Upper SaddleRiver, N.J: Prentice Hall, ISBN:0136097049 9780136097044.

[10] [9] Boneh D., 1999 “Twenty years of attacks on the RSA cryptosystem”, American Mathematical Society(AMS), Vol. 46, No. 2, pp. 203-213.

[11] National Institute of Standards and Technology, Data Encryption Standard (DES), Technical Report, Federal Information Processing Standards Publication 46-3, 1999.

[12] National Institute of Standards and Technology Advanced Encryption Standard (AES), Technical Report, Federal Information Processing Standards Publication 197, 2001.

[13] D. Hearn, M. P. Baker, Computer Graphics C Version (Second Edition, Prentice Hall, pp. 362-387).

[14] Kamal Gulat, Information Hiding Using Fractal Encoding (School of Information Technology Indian Institute of Technology Bombay,Mumbai, 2003).

[15] Fractal Cryptology, New Mexico High School, Supercomputing Challenge Final Report April 2,2003 , Team Members: Brandi Howell Anna Reese Michael Basile Team Sponsor: Paula AveryProject Mentor: Garth Reese.

[16] G. B. Huntress, Encryption using Fractal Key, United States Patent 6782101, 2004.

[17] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image Quality Assessment: From Error Visibility to Structural Similarity, IEEE Transactions on Image Processing, Vol. 13, No. 4, April 2004.

[18] Huntress G. B., 2004“Encryption using Fractal Key”, United States Patent 6782101.

[19] V. Rozouvan, Symmetry of the Modified Mandelbrot Set, Pi in the Sky, Pacific Institute for Mathematical Sciences (PIMS), Issue 9, December 2005.

[20] Zakeri, S., 2006 “On biaccessible points of the Mandelbrot set”. Proceedings of the AmericanMathematical Society, 134(8), pp 2239-2250.

[21] M. A. Alia, A. B. Samsudin, New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets, IJCSNS International Journal of Computer Science and Network Security, Vol. 7, No. 2, February 2007.

[22] Alia, M. A. and Samsudin A. B., 2007 “New Key Exchange Protocol Based on Mandelbrot and JuliaFractal Sets”, International Journal of Computer Science and Network Security, VOL.7 No.2.

[23] Q. Huynh-Thu, M. Ghanbari, Scope of Validity of PSNR in Image/Video Quality Assessment, Electronics Letters 44 (13), pp. 800-801, 2008.

[24] V. Rozouvan, Modulo Image Encryption with Fractal Keys, Optics and Lasers in Engineering, Vol. 47, issue 1, pp. 1-6, 2009.

[25] Jonathan F. “An Introduction to Julia sets”,2009.

[26] Y. Y. Sun, R. Q. Kong, X. Y. Wang, L. C. Bi, An Image Encryption Algorithm using Mandelbrot Set, International Workshop on Chaos Fractal Theory and its Applications, IEEE Computer Society, 2010.

[27] A. J. J. Lock, C. H. Loh, S. H. Juhari, and A. Samsudin, “Compression-encryption based on fractal geometric,” in Proceedings of the 2nd International Conference on Computer Research and Development (ICCRD'10), pp. 213–217, May 2010.

[28] A. J. J. Lock, C. H. Loh, S. H. Juhari, A. Samsudin, Compression-Encryption Based on Fractal Geometric, Second International Conference on Computer Research and Development, IEEE Computer Society, 2010.

[29] L. R. Knudsen, M. J. B. Robshaw, The Block Cipher Companion, Information Security and Cryptography, pp. 95-108, 2011.

[30] Zhang Q., Zhou S. and Wei X.,2011 “An Efficient Approach for DNA Fractal-based ImageEncryption”, Applied Mathematics & Information Sciences, 5(3), pp 445-459.

[31] P. Jhansi Rani, DurgaBhavani, Symmetric Encryption using Sierpinsky Fractal Geometry, International Conference on Information Processing, ICIP 2011 Proceedings, Springer-Verlag Berlin Heidelberg, pp. 240-245,2011.

[32] Motýl I., Jašek R., Vařacha P., 2012 “Analysis of the Fractal Structures for the InformationEncrypting Process”, International Journal of Computers, Issue 4, Volume 6, pp 224-231.

[33] W. Stallings, Cryptography and Network Security Principles and Practices (Pearson Education, 3rd edition).

[34] Abed F. S., 2011 “A New Approach to Encoding and Hiding Information in an Image”, IJCSIInternational Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, ISSN (Online): 1694-0814.

[35] B. Rama and J. Mishra, “Game-enabling the 3D-Mandelbulb fractal by adding velocity-induced support vectors,” International Journal of Computer Applications, vol. 48, no. 1, pp. 1–3, 2012

[36] Sun YY, Xu R., Chen L., Hu X., 2014 “Image Compression and Encryption Scheme Using FractalDictionary and Julia Set”, IET Image Processing, Vol. 9, Issue. 3, pp. 173–183 doi:10.1049/ietipr.2014.0224.

[37] Abd-El-Hafiz1 S. K., Radwan A. G.Haleem S. H. A., Barakat M. L., 2014 “A fractal-based imageencryption system”IET Image Processing, Vol. 8, Issue 12, pp. 742–752 doi:10.1049/ietipr.2013.0570.

[38] Sun Y, Chen L, Xu R, Kong R, 2014“An Image Encryption Algorithm Utilizing Julia Sets and HilbertCurves”. PLoS ONE, 9(1): e84655. doi:10.1371/journal.pone.0084655.

[39] Khan M. & Shah T., 2014“A Literature Review on Image Encryption Techniques”, © 3D ResearchCentre Kwangwoon University and Springer-Verlag Berlin Heidelberg, 5(4), DOI 10.1007/s13319- 014-0029-0, Page 1.

[40] S. K. Abd-El-Hafiz, A. G. Radwan, S. H. Abdel Haleem, and M. L. Barakat, “A fractal-based image encryption system,” IET Image Processing, vol. 8, no. 12, pp. 742–752, 2014.

[41] Abd-El-Hafiz1 S. K., Radwan A. G.Haleem S. H. A., Barakat M. L., 2014 “A fractal-based imageencryption system”IET Image Processing, Vol. 8, Issue 12, pp. 742–752 doi:10.1049/ietipr.2013.0570

[42] Sun YY, Xu R., Chen L., Hu X., 2014 “Image Compression and Encryption Scheme Using Fractal

[43] Dictionary and Julia Set”, IET Image Processing, Vol. 9, Issue. 3, pp. 173–183 doi:10.1049/ietipr. 2014

[44] SomarajS. and Hussain M. A., 2015 “Performance and Security Analysis for Image Encryption usingKey Image”, Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/73141.

[45] Negi D., Negi A., Agarwal S., 2016 “The Complex Key Cryptosystem”, International Journal ofApplied Engineering Research, ISSN 0973-4562 Volume 11, Number 1, pp 681-684.

[46] Ali M. Meligy, HossamDiab, Marwa S. El-Danaf,2016“Chaos Encryption Algorithm using KeyGeneration from Biometric Images”, International Journal of Computer Applications (0975 – 8887)Volume 149 – No.11.

[47] Wang W., Tan H., Pang Y., Li Z., Ran P. and Wu J.,2016 “A Novel Encryption Algorithm Based onDWT and Multichaos Mapping”, Hindawi Publishing Corporation Journal of Sensors Volume Article ID 2646205, 7 pages,http://dx.doi.org/10.1155/2016/2646205.

[48] Kashanian H., Davoudi M. and Khorramfar H., 2016 “Image Encryption using chaos functions andfractal key”, International Journal of Advanced Biotechnology and Research (IJBR) ISSN 0976-2612,Online ISSN 2278–599X, Vol-7, Special Issue-Number4, pp1075-1082.

[49] Shafali Agarwal, IMAGE ENCRYPTION TECHNIQUES USING FRACTALFUNCTION: A REVIEW, International Journal of Computer Science & Information Technology (IJCSIT) Vol 9, No 2, April 2017.