IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903073 |

Security and Restoration on Image Processing using Wavelets and Fuzzy Logic

Dr.V V Teresa, Naveena M, Lakshmi Priya R.G, Prakash R, Praveen R

Associate Professor, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

UG Student, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

UG Student, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

UG Student, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

UG Student, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

ABSTRACT: The biggest technological events of the last decades were the violation of the digital media during a whole range of lifestyle appearance. Copying is simple without lossless of fidelity and a reproduction of a digital media is simply just like the first. With digital multimedia distribution through global networks ownership (IPR) are more threatened than ever thanks to the likelihood of unlimited copying, therefore the security is that the most problem within the modern digital world. Users should reduce permissions and access rights of applications and users as a solution to these security threats by packing up unused resources, keeping safety gaps updated, and reducing permissions and access rights of applications and users. Cryptography is often used as another approach to this issue. Cryptography is made up of two parts: cryptology and cryptanalysis. Cryptology includes encryption. It's the tactic of converting a readable message/image into an unreadable format by employing a group of rules for that process. it's called an encryption algorithm. The vast majority of these days existing encryption calculations concern just on security This concept of encryption is implemented on images as an area of multimedia by using multi objective soft computing algorithms like mathematical logic and fuzzy sets. Soft computing technology may also refer to a branch of computing that is characterised by the use of ad hoc solutions to computationally difficult tasks such as solving complete problems. Furthermore, it is being described as a fusion of methodologies designed to model and allow solutions to world problems that are not modelled or too difficult to model mathematically. Its aim is to require advantage of the leniency for imprecision, doubt, approximate reasoning, and partial truth so on realize close resemblance with human like deciding. The soft computing methodology has been exercised successfully to the solution of the various heavy computation problems, mainly within the fields of image processing and video processing. Very interesting and promising results.

KEYWORDS: Fuzzy logic, Wavelets, Encryption, Decryption, Fuzzy sets, Image Enhancement, Cryptography

I. INTRODUCTION

Many problems of data security and privacy increase every day with the existence and development of computer networks. Obtaining a safe and effective system for communicating with photographs has become a requirement, and the issues surrounding it must be carefully considered. As a result, network encryption and authentication became critical. Digital images are one of the most useful forms of knowledge. Image encryption is used in a variety of areas, such as multimedia systems and Internet communication, medical imaging, military communication and telemedicine [1-3]. There are two types of applications for transporting information over the World Wide Web: The online applications, which consider the speed as the main issue. The web pages, which consider the security as the main issue. [4-5] This thesis introduced three approaches of image encryption to improve the conventional encryption algorithms and to fulfill the requirements of these two applications, which were studied and adjusted to meet the requirements of image encryption. The vast majority of the accessible encryption calculations are utilized for text information. Algorithms that work well with textual data can not work well with multimedia data due to broad data sizes and real-time constraints. 6 – 9 Despite the fact that the triple-data encryption standard (T-DES) and the international encoding algorithm (IDEA) provide high protection, they are not suitable for multimedia applications. The encoding standard (DES), advanced encryption standard (AES), and international encoding algorithm (IDEA) are all text encryption algorithms. [10, 11] Although we will use the normal encryption algorithms to encrypt images directly, this might not be an honest idea for 2 reasons. For instance, photographs are usually larger than text. Second, the decrypted text must

be sufficient in comparison to the original. This condition is not mandatory for image data due to the essence of human interpretation. In most cases, a decrypted image with minor distortion is sufficient. [12] The connection among the image elements in a given arrangement is responsible for the information presented in an image. This recognizable data are regularly diminished by diminishing the relationship among picture components utilizing certain change strategies. [13] In addition, encryptions techniques are becoming significantly more sophisticated and have been widely used with the increasing use of Internet and other efficient communication techniques, the copyright protection furthermore, verification of advanced substance have acquired extraordinary significance. Image is very sensitive to any alterations required for cryptography embedding. Text, audio, image and video have inherent redundancies which are compatible with the limitations of human visual and auditory systems that we can utilize for cryptography embedding.
Copyright insurance, content authentication, and image report alter identification have all recently become a legitimate concern for analysts. Furthermore, research on image security schemes over the last decade has primarily focused on copyright protection, with less attention paid to lossless data, content authentication, integrity verification, tamper detection, distortion, and speed. Detecting random tampering attacks, the encryption capacity, complexity and robustness need extra cipher information and a modification of the original plain image to embed the cipher information. All of that was not considered by the traditional encryption techniques that have been proposed and still the main issues of content authentication, integrity verification, real time and tamper detection of image documents. On the other hand, the security of legal, financial, sensitive and critical image is still an obstacle in the technology of information exchange via Internet for various applications and purposes. This research presents new intelligent approaches based on combination of soft computing algorithms and natural image processing techniques for content authentication and tampering detection of image.[12]

II. RELATED WORK

Sanchez et. al. [16] have proposed 3-D adaptable pressure technique for clinical pictures upheld the enhanced 14 Volume Of Interest (VOI) coding. In which distinctive far off customers may gain admittance to the compacted 3-D clinical imaging information put away on a focal worker. This method performs 3-D integer wavelet transform and an altered Embedded Block Coder with Optimized Truncation (EBCOT) with 3-D settings for making a versatile piece stream. This upgraded VOI coding was acquired by a streamlining method which reorders the yield bit-stream subsequent to encoding. Hence the bits belongs to VOI are decoded with greater quality. This Bit-stream reordering system was upheld the weighting model which consolidates the situation of the VOI and mean energy of the wavelet coefficient.

Sanchez et. al. [17] have proposed a symmetry-based technique for scalable lossless compression of 3-D medical image of knowledge which employs 2-D integer wavelet transform to decorrelate the info, likewise an intraband forecast technique for decreasing the energy of the sub-groups. The adjusted EBCOT, customized as per attributes of information, encodes the leftover information created after the expectation to supply goal and quality adaptability. Zuo-Dian et. al. [18] have advanced a technique for lossless clinical picture coding called Adaptive Predictive Multiplicative Autoregressive (APMAR). The APMAR was wont to improve the accuracy of prediction in encoded image blocks. Here, each square was adaptively anticipated by one of the seven indicators of the JPEG lossless mode and neighborhood mean indicator. The lingering esteems were prepared by the multiplicative autoregressive model with Huffman coding.

Chen et. al. [19] have developed a model with multiple context and arithmetic coding to enhance the performance of the 15 compression. Two quantizers were used with a large number of quantization stages during the implementation. This involves many resonance (MR) and Ultra Sound (US) images. The usage of multiple contexts has improved the performance of the compression by 25% to 30% for MR images & 30% to 35 % for US images. Nijim et. al. suggested a method for evaluating and comparing the efficiency of the lossless linear predictor and the lossless Joint Photographic Experts Group (JPEG) norm for lossless compression of MR and US pictures. The benefits were the computational intricacy was extraordinarily diminished and the coefficients of the differentiator were known by the encoder and decoder.

Wang et. al. [5] have proposed a 3D medical image compression for a low complexity Reversible Integer Karhunen-Loe Transform (RKLT) which is used for exploiting the correlation by integer wavelet transform in the spatial domain. As the result of this the low RKLT provides comparable lossless compression performance. Gruter et al. (2000) suggested a decomposition method for the Morphological Subband Decomposition's creation and generalisation (MSD). It is proved that the Rank Order Polynomial Decomposition (ROPD) has a better lossless rate than the MSD. The possibility of hybrid lossless compression has been done by using ultrasound images. Das et. al. (1993 and 1994) have put forth a method for lossless predictive coding using 2D space varying least squares model for medical image. This method's efficiency was compared to that of the current technique Hierarchal Interpolation (HINT).The author has also proposed a model namely multiplicative auto 16 regressive model for 2D medical images. Both the proposed schemes achieved the higher compression rate.

III. PROPOSED ALGORITHM

The soft computing algorithms are the fusion of paradigms designed to present solutions to the real- world problems, which are not modelled or very difficult to be modelled mathematically. They are a set of methodologies that work together synergistically to provide versatile knowledge and processing capabilities for dealing with real-life uncertain circumstances of one type or another. Their aim is to take advantage of people's tolerance for imprecision, ambiguity, reasoning, and partial truth in order to achieve a near resemblance to human decision-making. Soft computing is an optimization method for finding solutions to difficult-to-solve problems. Fuzzy sets theory is one of the most important branches of soft computing algorithms. Fuzzy sets were introduced by Lotfi A. Zadeh in 1965 to represent data and knowledge possessing non-statistical uncertainties. Fuzzy logic is an approach related to the fuzzy sets theory of soft computing algorithms based on “degree of truth” rather than the usual “true of false” (1 or 0) and Boolean logic on which the fashionable computer is predicated This paper introduces two new image encryption algorithms that make use of fuzzy set theory to provide high protection for image data against unauthorised intrusions. Within the encryption and decryption processes, it is fast.It is fast within the process of encryption and decryption. The decryption process does not result in any image data loss, and it can also handle various image formats. By generating random sequences for the encryption/decryption process, the first algorithm used symbolic logic to supply security levels and their corresponding processing levels. The second algorithm based on fuzzy graph to obtain highly encrypted image.
The fuzzy sets theory is a theory that deals with groups of objects that have non-sharp boundaries and whose membership is determined by degree. Since 1992, the fuzzy set theory is known as the theory of neural nets and the field of evolutionary programming have become one of the important areas of ‘computational intelligence’ or ‘soft computing’. The deep bond that exists between these two areas has naturally grown closer. In this section, however, the focus primarily will be on the notion of fuzzy set theory, fuzzy logic and fuzzy graph. The notion of a fuzzy set stems from the observation made by Zadeh (1965a) that “more often than not, the classes of objects encountered within the real physical world don’t have precisely defined criteria of membership”.

Fuzzy logic is brilliant engineering and data analysis approach proposed by Lotfi A. Zadeh. This section deals with the basic concept of fuzzy logic, and it includes some basic examples of fuzzy logic. The modern machine is focused on fuzzy logic, which is an approach based on "degrees of fact". In addition, the fuzzy logic has two different meanings; one is wide and the other is narrow.

In a broad sense, fuzzy logic (FL) is almost identical to fuzzy set theory. The narrow sense, on the other hand, depicts fuzzy logic as a logical structure that is an extension of multi-valued logic. In this light, symbolic logic in its narrow sense may be considered a subset of FL. Even in its more narrow definition, symbolic logic differs both in concept and nature from traditional multi-valued logical systems. Azriel Rosenfeld suggested fuzzy graph theory in 1975. tho' he was terribly young, he has been growing quick and has varied applications in numerous fields . Later on, Bhattacharya [155] discussed fuzzy graphs. Mordeson and Peng, for example, implemented several fuzzy graph operations. E. Sampathkumar introduced a new definition called graph structure.

A fuzzy graph is a pair in which is a symmetric fuzzy relation on and is a fuzzy subset of S. The vertices or nodes of G are called the elements of S, and the pair of vertices are called edges in G. The fuzzy graph's underlying crisp graph is denoted by G*: (S, E), where the crisp graph (S, E) may be called a version of the fuzzy graph G, with each vertex and fringe of (S, E) having a degree of membership.

3.1 Mechanism of Fuzzy Logic

The use of fuzzy logic needs at least two input magnitudes. If they are more, they would be better for fuzzy logic. Three basic steps are needed for applying fuzzy analysis:
- ❖ Fuzzification of the inputs
- ❖ Fuzzy-Inference
- ❖ Defuzzification of obtaining crisp output

For fuzzification, a fuzzy set is required for each input. This set is a kind of linguistic variables such as relative terms: far, close, small, normal, high, cold, warm, hot, etc. Once fuzzy set is defined for each of the variables, the degree of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903073 |

membership should be calculated for every input. Minimum degree of membership is zero, and maximum is 1 or 100%. To calculate degree of membership, it is easy to use linear functions as presented in figure 1

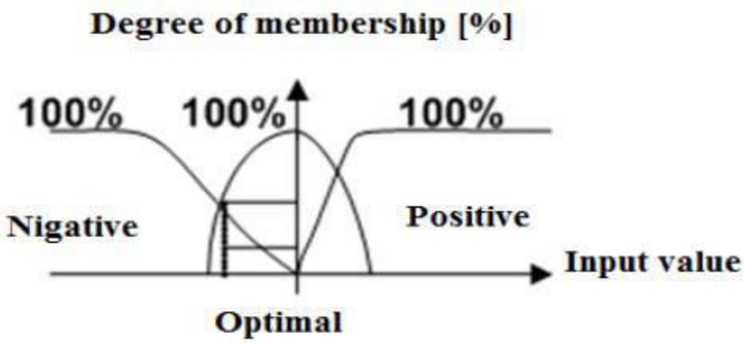

Figure 1 Calculation degree of membership using Gaussian function

After calculating the degrees of membership for every input and every fuzzy set, the step of (fuzzy-inference) should be started. All numerical data obtained in fuzzification process need to be mutually compared in 'if-then' fashion. This process is called fuzzy-inference. Overall range of 'if-then' rules is up to the outputs of

fuzzy set numbers for each input. For example, if we have two input values; input X has three fuzzy sets (negative, optimal and positive), and input Y has five fuzzy sets (negative, negative-optimal, optimal, optimal-positive and positive), the (15) 'if-then' rules square measure needed to check negative degree of membership of X with negative degree of membership of Y, negative degree of membership of X with negative-optimal degree of membership of Y then forth.In fact, there is a need for comparing at least two numbers in every 'if-then' rule, but there are a lot of numbers and 'if-then' rules to be compared. There are various options to show how to determine output from compared numbers in each 'if-then' rule. Options are as follows:

- Choose minimum: $\mu=\min\{X, Y, Z\}$
- Choose maximum: $\mu=\max\{X, Y, Z\}$
- Choose complement $\mu C = 1-\mu$

Defuzzification is used for obtaining crisp output from numbers obtained in step fuzzy-inference. In order to calculate crisp output, we can use "centre of gravity" or some other method. Together with numbers from fuzzy-inference, we need to have additional parameters called "singleton values". Singleton values can be achieved from experiments

eq.(3)

IV. SIMULATION AND RESULTS

The In this section, several experiments are performed to test the effect of the proposed algorithms on image encryption. The proposed approaches are implemented and applied to three images, which have different types and sizes, to verify its adaptability, quality, security and speed. The results are illustrated in this section to confirm the properties of proposed approaches based on genetic algorithm and to compare them with the quality of image encryption. The security analysis performed in this approaches is visual analysis, histogram analysis, correlation coefficient. All these experiments prove that the proposed approaches in this chapter fulfil all the results completely and rightly. In this subsection, the discussions and analyses of the encryption algorithms based on fuzzy logic and fuzzy graph are presented. The following discussions and analyses are performed on original, encrypted and decrypted images. In these experiments, the algorithm parameters are set as follows: the images sizes are different; the length of images blocks is (48×48) pixels in fuzzy logic and (8×8) pixels in fuzzy graph. Image cryptography and cryptography tests are allotted victimisation commonplace pictures of various sizes in grey scale and color.

Encrypted and decrypted outputs have been obtained from fuzzy logic and fuzzy graph algorithms. It may be n oted that the encrypted image obtained from fuzzy logic and fuzzy graph algorithms does not resemble the original image.

The execution time of encoding and cryptography method by planned approaches based on genetic algorithms has been implemented and conducted using Matlab- 7.10.0 (R2010a) in AMD V 140 CPU @ 2.30 GHz with Windows-7 operating system. In this case, three separate images having the different type's formats of JPG, TIF and BMP respectively and sizes 225 × 225 pixels, 194 × 259 pixels and 1153 × 2050 pixels have been used to measure the encryption time for each image by using the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |
|| Volume 9, Issue 3, March 2021 ||
| DOI: 10.15680/IJIRCCE.2021.0903073 |

suggested approaches. The encryption time obtained using these images are given in tables 5.7. The average time of encryption is achieved by fuzzy logic and fuzzy graph while encrypting different images of different sizes and formats. This shows that the fuzzy graph algorithm is 1.07 times less than fuzzy logic algorithms.

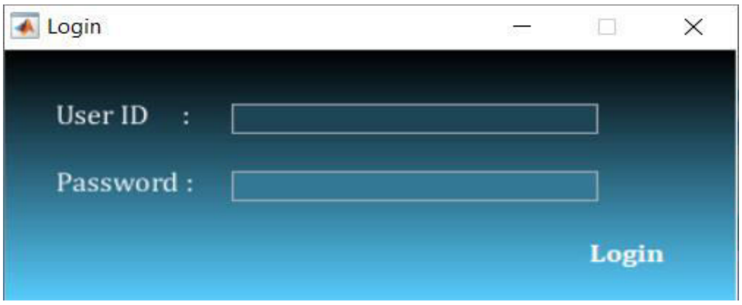

Figure 2 Login Details

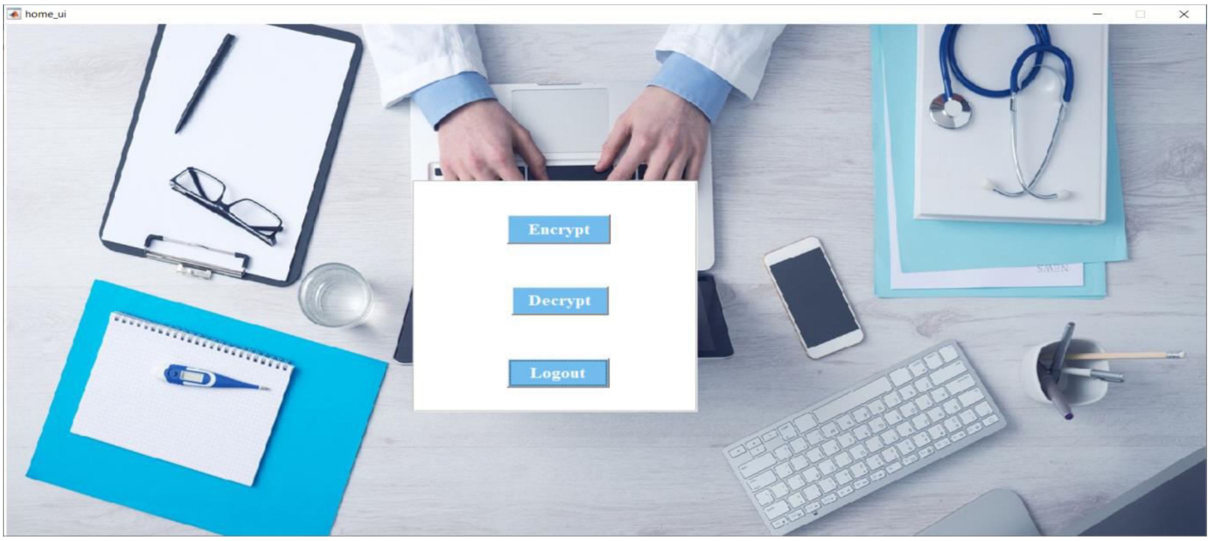

Figure 3 Login Page

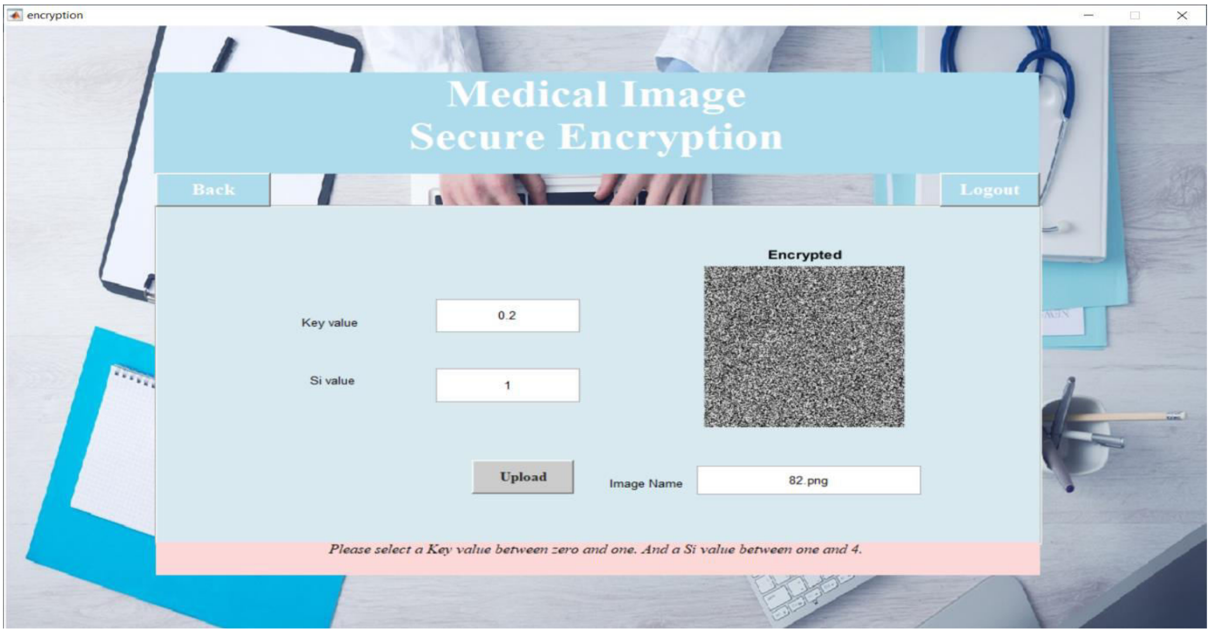

Figure 4 Encrypted Image

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903073 |

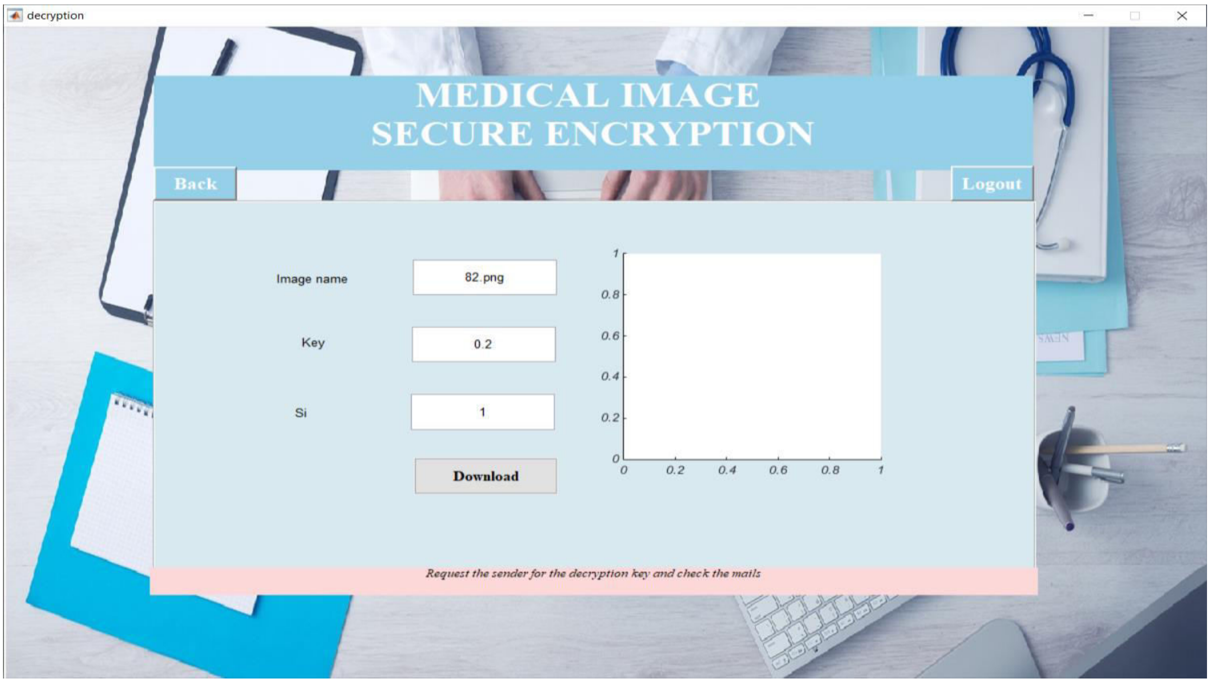

Figure 5 Decrypted Image

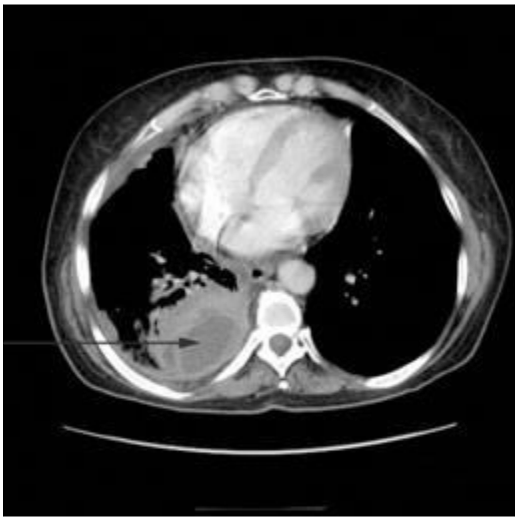

Figure 6 Final Extracted output

Average time of encryption and decryption by using fuzzy logic and fuzzy graph algorithms with Three Different Images

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903073 |

Average time of encryption and decryption by using fuzzy logic and fuzzy graph algorithms with Three Different Images		
Image / Approach	Fuzzy Logic	Fuzzy Graph
Lena	16.477	14.936
Bird	15.741	14.525
Car	56.645	53.812

V. CONCLUSION AND FUTURE SCOPE

Designing an encryption algorithm, specifically for image data, which has low bit rate overhead due to encryption, maximum security, minimum lossless, high speed, and realizable computational complexity is not an easy task to accomplish. There are a number of different methods proposed for image encryption in the literature, but some of these methods could not satisfy all the desired requirements. In this thesis new methods are proposed based on pixels system and soft computing algorithms (genetic algorithms and fuzzy sets theory) for image data encryption, which is robust to the intermediate bit rate conversion operation and which has an adjustable security level and operate with slight bit rate overhead. The main focus of this thesis was to improve the quality, security and speed of image encryption and to develop novel approaches of encryption based on soft computing algorithms (genetic algorithms and fuzzy logic algorithm). The research work described in this thesis has been concerned with the designing of new multiple and multiobjective encryption algorithms for the enhancement of image security. A number of significant features of the proposed multiple and multiobjective encryption algorithm have been described. The effectiveness and robustness of the proposed algorithms have been demonstrated. They can supply sufficient security against various security threats. These approaches are playing an important role in modern encryption algorithms to keep image security

REFERENCES

[1] O. S. Faragallah, "Utilization of Security Techniques for Multimedia Applications", Ph. D. Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2007.
[2] A. J. Menezes, P. C. V. Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press Boca Raton, USA, 1996.
[3] L. Qiao, "Multimedia Security and Copyright Protection", Ph.D. Thesis, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, Illinois, USA, 1998.
[4] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice- Hall Upper Saddle River, USA, 1999.
[M. B Ayman. Albassal, Abdel-Moneim and A. Wahdan, "Genetic Algorithm Cryptanalysis of a Feistel Type Block Cipher", International Conference on Electrical, Electronic and Computer Engineering, Egypt, PP. 217 – 221, 2004.
[6] D. Stinson, "Cryptography: Theory and Practice", Second edition, Chapman & Hall / CRC Boca Raton, USA, 2002.
[7] Y. Mao, G. Chen and S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", International Journal of Bifurcation and Chaos, Volume14, Issue10, PP. 3613 – 3624, 2004.[8] S. Li, "Analyses and New Designs of Digital Chaotic Ciphers", Ph. D. Thesis, School of Electronics & Information Engineering, Xi'an Jiaotong University, China, June 2003.
[9] National Bureau of Standards, "Data Encryption Standard Modes of Operation", Federal Information Processing Standards Publication 81, US Government Printing Office, Washington D. C, 1980.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903073 |

[10] L. Jubairahmed, S. Satheeskumaran, and C. Venkatesan, "Contourlet transform based adaptive nonlinear diffusion filtering for speckle noise removal in ultrasound images," Cluster Computing, vol. 22, no. S5, pp. 11237–11246, Nov. 2017.

[11] L. J. Ahmed, "Discrete Shearlet Transform Based Speckle Noise Removal in Ultrasound Images," National Academy Science Letters, vol. 41, no. 2, pp. 91–95, Apr. 2018.

[12] G. Rajesh Hien Dang, K. Martin Sagayam, S. Dhanasekar,"Image Fusion based on Sparse Sampling Method and Hybrid Discrete Cosine Transformation",International Journal of Scientific and Technology Research,vol.8,no.12,pp.1103-1107,December 2019.

[13] J. Anitha S. Dhanasekar, P. Malin Bruntha, S.Immanuel Alex Pandian,"Local Ternary Co-occurrence Patterns based Lung Nodules Detection",2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS),pp.489-492.