

## ADVANCED ENCRYPTION USING FUZZY LOGIC AND SECRET SHARING SCHEME

Joseph James S<sup>1</sup>, S.Selvakumara Samy<sup>2</sup>, Haribaabu V<sup>3</sup>  
 ASST.PROF (O.G)<sup>1, 2, 3</sup>, SRM Institute of Science and Technology  
<sup>1</sup>Josephjames.s@ktr.srmuniv.ac.in

**Abstract:** This research paper introduces Encryption and Decryption using fuzzy logic and  $(n, n)$  secret shares using fuzzy logic. The meaning of fuzzy is vague, ambiguous and uncertain. Encryption and decryption methods using fuzzy logic will be difficult to guess. Hence secret sharing concept using fuzzy logic is better and enhanced method of encoding of data for more security. Visual cryptography is a technique of encryption to embed secret messages in an original image therefore the secret messages can be decrypted by the human view with requiring not much calculation. The  $(n, n)$  secret hiding scheme provides more security and confidentiality. In secret hiding, share images are constructed based on fuzzy logic and user desired input. The  $(n, n)$  secret sharing scheme divides information into  $n$  shares. During decryption the  $n$  shares are brought together recreate the secret information.

**Keywords:** Secret hiding, Shares, FuzzyLogic, Visual secret sharing, Data Encoding.

### 1. Introduction

Information Encryption and Decryption here means security. Fundamentally Security is to secure the information from the unapproved individual or any group. Information change implies sending any sort of data from source to goal without the loss of the information. Presently a day the issue in information exchange is security. Essentially information security isn't something that we can get, it is something that we do. A Fuzzy Logic is utilized for Encryption and mystery shares. Encoding will give an answer for the security of information.

The purpose behind actualizing an encryption-decoding framework is protection. As data goes over the World Wide Web, it winds up defenseless against access from unapproved people or associations. Accordingly, information is encoded to anticipate information misfortune and burglary. Barely any things will be scrambled that are email messages, content documents, pictures, client information and catalogs. In goal side, the individual responsible for unscrambling gets a provoke or window in which a secret word might be entered to get to scrambled data. Encryption is the

strategy for encoding data or messages such that lone approved individual can read it. Data encryption process does not forestall capture attempt, but rather keeps the message content from the interceptor. In an encryption procedure, the expected data or message, alluded to as plaintext, is encoded utilizing an encryption calculation and creating figure message that can be perused just if unscrambled. The prevalent information scrambling technique utilizes AES calculation of 128 bits, 192 bits, 256 bits. For specialized reasons, an encryption procedure as a rule utilizes a pseudo-irregular encryption key produced by key creating calculation. It is conceivable to unscramble the message without having the key, be that as it may, for all around composed encryption techniques, huge computational assets and expertise are required. An approved beneficiary can without much of a stretch translate the data with the key gave by the key generator to beneficiaries, however not to unapproved interceptors.

The objective of encryption is to ensure that exclusive the individuals who are approved to get to information (e.g. an instant message or a record) will have the capacity to peruse data, utilizing the gave unscrambling key. The individuals who are not approved can't get to the message, since he or she doesn't have the required key, without which it is computationally difficult to peruse the scrambled message.

Decoding is the technique for changing information that has been gotten muddled through encryption back to its plaintext frame. In unscrambling, the framework concentrates and changes over the information it to its individual plain messages and pictures that are effortlessly reasonable by the per user and furthermore by the framework also. Unscrambling might be accomplished physically or consequently. It might likewise be performed with an arrangement of keys or passwords.

In our proposed work, we have changed over client secret word into a key and afterward we utilized that key for encryption and decoding. In this work  $(n, n)$  visual secret concealing plan is utilized to exchange classified information through picture that is fluffy rationale based encryption. In  $(n, n)$  mystery concealing plan  $n$  share pictures will be produced with reference to

the first picture. Also, fluffy rationale will be helpful to offer significance to information and make the encryption more grounded. And furthermore fluffy rationale makes encryption and decoding hard to figure and message is more secure.

## 2. Experiment

### A. Encryption Scheme

The Encryption plot utilizes AES calculation for encryption of documents. AES utilized as a part of our paper is of 128 bits, 192 bits, 256 bits. At the point when the client presents its document alongside the secret word then the encryption conspire calls the fluffy rationale to get the AES encryption bits (128,192,256). At that point it calls the encryption key generator to create a key of the required bits. After that the encryption conspire begins the encryption procedure. In this strategy, it's exceptionally troublesome for the aggressor to know which bit AES was performed. Additionally the key age depends on randomization so it's difficult for assailant to know the key.

### B. Fluffy Encryption Logic

The Fuzzy Encoding rationale is a critical thinking technique that can be actualized in assortment of frameworks extending from basic, installed microcontrollers to vast, multichannel. Principles and enrollments sets are used in this fluffy encryption to decide. To give security from different assailants, the calculation it utilizes distinctive key factors and qualities. The fluffy encryption chooses which bit AES ought to be utilized. It restores the esteem which the encryption key generator uses to create a key of the specific bits as recommended by fluffy encryption rationale.

### C. Mystery Hiding Scheme

Mystery covering up is additionally called as mystery isolating strategy. Easiest case of mystery stowing away is secret word part to provide watchword as greater security. Thought about an illustration, solid passwords are difficult to remember. A client will a (n, n) mystery concealing plan to create a two offers for a given watchword and he will store one offer in his in bank store sheltered and other one in individual book. On the off chance that one day the client overlooked his secret key, he can recover the watchword effortlessly. On the off chance that mystery concealing plans are utilized, the thought behind this is, the assailants need to take numerous offers from a wide range of spots. In mystery concealing plan a mystery is shared among a gathering of individuals. Every member is allotted an offer of the mystery. Mystery concealing plans are utilized for putting away data that is profoundly

delicate and exceptionally essential for classified data exchange like encryption keys, rocket dispatch codes, and numbered ledgers. Every one of these snippets of data must be kept exceedingly secured, since their introduction could be misfortune for somebody essential data.

### D. Fluffy Dividing Logic

The Fuzzy partitioning rationale is a strategy for multi esteemed rationale created from fluffy set hypothesis to give thinking that is suitable as opposed to settled. The Fuzzy Splitting is utilized to set the scope of mystery shares. At that point the client has an alternative to pick the quantity of offers from inferred extend. The scrambled picture which contains the mystery information is then splitted in view of the range and the esteem picks by the client. Fluffy means indeterminate and uncertain. In this day and age fluffy rationale is one of the registering instruments and it is likewise connected by numerous encryption calculations.

### E. A (n, n) Visual Cryptography Scheme

A (n, n) visual mystery concealing plan produces n shares pictures from a scrambled picture and including n shares together gives an encoded picture. The (n, n) visual mystery sharing plan partitions the mystery picture or record content into n shares so reproduction of mystery picture or document content from an offer is unimaginable. Here in (n, n) visual mystery sharing plan, it isolates the mystery picture or record content into n shares. For instance a mystery picture is to be shared among two members since it is (n, n) mystery concealing plan. The picture is isolated into n shares with the goal that when n shares are included it is unmistakable. At the point when not as much as n shares are included, the mystery stays undetectable.

### F. Decoding Scheme

Decoding is the strategy for changing over information that has been gotten confused through encryption process back to its plain content frame. In decoding, the framework concentrates and changes over the data and changes it to writings and pictures that are effectively justifiable by the framework and the peruser too. The Decryption procedure does decoding on the collector side. The Decryption technique recovers the first mystery picture from created shares. The offers contain every one of the points of interest which are expected to begin the unraveling procedure. The scrambled offers are recovered and after that in view of the key the procedure begins. Thus the first picture or document is downloaded on the beneficiary end.

### 3. Methodology

Stepwise flow of proposed work on Sender Side:

Step 1: Login or Signup

In order to submit the files, login is mandatory. Login helps in identifying the sender and the receiver.

Step 2: Enter confidential data along with password

The file is submitted after login along with the password. The password is necessary which is used to generate the key.

Step 3: Fuzzy Encryption Login

The Fuzzy contains some rules and memberships sets which decide the AES bit needs to be performed on the file.

Step 4: Key Generator

The key generator receives a value from fuzzy encryption logic and that based on that it will generate one key from the following bits: 128 bits, 192 bits, and 256 bits.

Step 5: Encryption Algorithm

Encryption is a technique of making an original message unreadable with an encryption algorithm. The encryption algorithm is a combined work of data encryption and decryption process. It provides high security to the information that are transmitted. File is encoded using a secret key.

Step 6: Image Creation

The data from the encrypted file is stored in a blank image. The width and height of image is 256 x 256

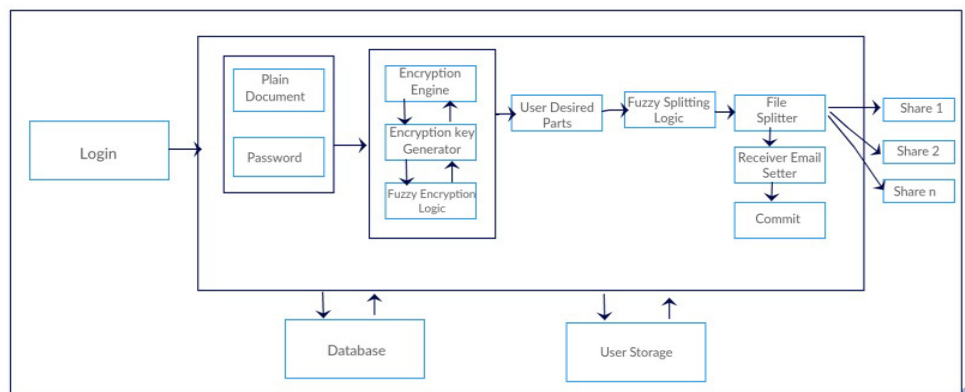


**Figure 1.** Secret share generation process

Step 7: Fuzzy Splitting Logic

The Fuzzy Splitting Logic is used to generate the range for secret shares. To achieve security from various attackers, the algorithm uses different key variables and values. The user will then choose a value from the derived range.

Step 8: Secret Shares

Based on fuzzy logic and user value the shares of the encrypted image is formed and saved into the internal storage of the server.

Step 9: Receiver Email - Id

The Receiver email id is then submitted so that when receiver get back then he will start the Decryption process and download that file.

Stepwise flow of proposed work on Receiver Side:

Step 1: Login or Signup

In order to submit the files, login is mandatory. Login helps in identifying the sender and the receiver.

Step 2: Sender Email – Id

The Receiver will enter the sender email from which it has to receive the file and then our server will merge the shares and decrypt the file. The receiver will then able to download the original file

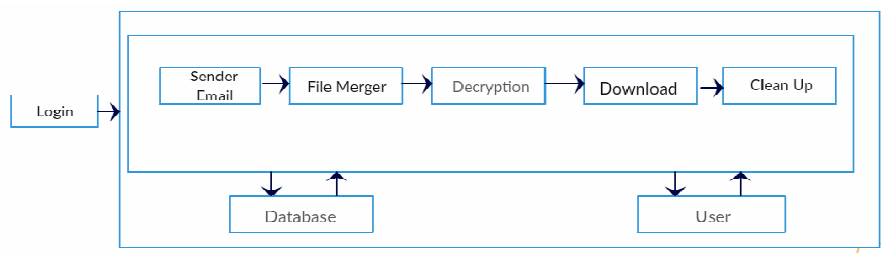


**Figure 2.** Process of regenerating original image from share

#### 4. Result and Discussion

In this research work, we took secret word file content and one image for encryption. During encryption

process four secret shares were generated by referring secret file content and original image.

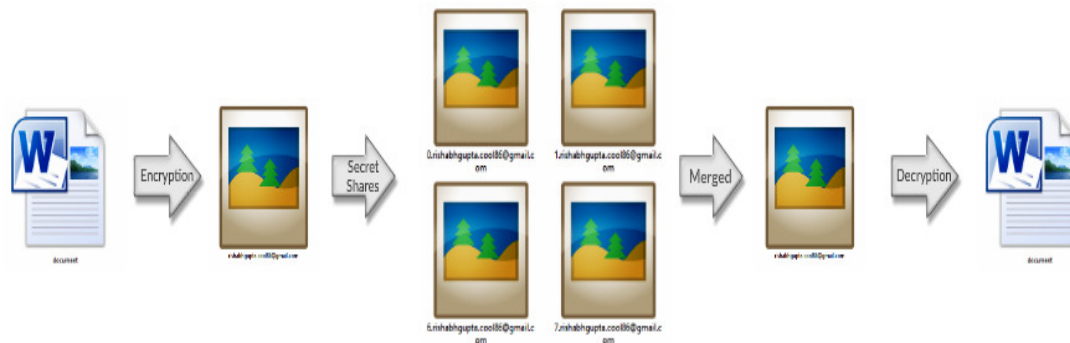


**Figure 3.** Secret File, original Image, Secret Shares and Decrypted Secret File

These generated secret share images will not reveal anything, since the intruders can view the pixel values of shares in numeric. Our of four secret shares, at least two shares are needed in order to get secret file content through decryption process otherwise secret file content cannot be retrieved from the encrypted shares.

#### 5. Conclusion and Future Work

In this paper, mystery document encryption depends on fluffy rationale for mystery message exchange utilizing  $(n, n)$  mystery concealing plan. To give the confirmation  $(n, n)$  mystery concealing plan is utilized. The information encryption procedure is simple yet information inside picture and afterward picture encryption in view of fluffy rationale and mystery covering up is something else which is exceptionally hard to split. This ordinary system gives greater security, privacy and honesty to the mystery message from unapproved individual. Mystery concealing plan with Fuzzy rationale, makes encryption and unscrambling strategy hard to split. So the information is more secure. To look after honesty, fluffy rationale alongside mystery concealing plan gives improved method for picture and mystery message encryption for private information exchange. Preferred standpoint of our proposed technique is, the encryption and unscrambling strategies are computationally less difficult yet the encoded picture is elusive mystery message or to discover any example in it. Unique picture debasement is inescapable due mystery share age and interpreting utilizing mystery shares. Typically mystery share are four times greater than unique pictures. In future we decrease picture corruption and significant mystery shares age.

#### References

- [1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption", World Academy of Science, Engineering and Technology 27 2007, pp. 206-211.
- [2] Yicong Zhou, Karen , Sos Agaian, "Image Encryption Using Binary Key- images", Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009, pp. 4569-4574.
- [3] In Koo Kang, Gonzalo R. Arce and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", 978-1-4244-2354- 5/09/©2009 IEEE, pp. 1473 -1476.
- [4] B. K. Shreyamsha Kumar and Chidamber R. Patil, "JPEG Image Encryption using Fuzzy PN Sequences", Signal, Image and Video Processing, Vol. 4, No. 4, pp. 419-427.
- [5] Siddharth Malik, Anjali Sardana and Jaya, "A Keyless Approach to Image Encryption", in 2012 International Conference On Communication Systems and Network Technologies, pp. 879-883.
- [6] Divya James and Mintu Philip, "A Novel Anti Phishing framework based on Visual Cryptography", 978-1-4673-0449-8/12/ \$31.00 © 2012 IEEE.
- [7] Kulvinder Kaur, Vineeta Khemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption", 978-1-4673-4529-3/ 12/ \$31.00c 2012 IEEE , pp. 1108-1113.
- [8] Yi-Jing Huang1 and Jun-Dong Chang, "Non-expanded Visual Cryptography Scheme with Authentication", IEEE 2nd International Symposium

on Next-Generation Electronics (ISNE) -February 25-26, Kaohsiung, Taiwan, pp-165-168.

[9] N. Askari, H.M. Heys, and C.R. Moloney," An Extended Visual Cryptography scheme without Pixel Expansion for Halftone Images", 2013 26th IEEE Canadian Conference of Electrical And Computer Engineering (CCECE).

[10] Anurag Mohapatra, Madhabananda sahuo, Ashis Kumar Mishra, "Message Security And Integrity Maintenance Using Fuzzy Logic And Secret Sharing ", in International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 ISSN 2229-5518, pp. 1055-1058.

[11] Gamil R.S. Qaid1, Sanjay N. Talbar," Encrypting Image by Using Fuzzy Logic Alogrithm", International Journal of Image Processing and Vision Sciences (IJIPVS), ISSN (Print): 2278 – 1110, Vol-2, Iss-1, 2013, pp. 25-29.

[12] RatnaBabu, M.Sridhar, Dr. B. RaveendraBabu," Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm For Visual Information Security", 978-1-4673-5986-3/13/\$31.00 © 2013 IEEE , pp. 195-199.

[13] ShyongJianShyu, "Threshold Visual Cryptographic Scheme with Meaningful Shares", in Ieee signal processing letter, vol, 21, NO.12, december2014, pp. 1521-1525.

[14] Hirdesh Kumar, AwadheshSrivastava, "A Secret Sharing Scheme for Secure Transmission of color images", 978-1- 4799- 2900-9/ 14 / \$31.00 © 2014 IEEE, pp. 857-860.

[15] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g", International Journal of Pure and Applied Mathematics, ISSN NO: 1314-3395, Vol-115, Issue -8, Sep 2017.

[16] S.V. Manikanthan, T. Padmapriya "An enhanced distributed evolved node-b architecture in 5G telecommunications network" International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254.March2018.

[17] S.V. Manikanthan, T. Padmapriya, Relay Based Architecture For Energy Perceptive For Mobile Adhoc Networks, Advances and Applications in Mathematical Sciences, Volume 17, Issue 1, November 2017, Pages 165-179.

