iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42262

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

A Survey Paper Based On Image Encryption and Decryption Technique

Kajal G. Shahare[1], Prof. Jayant Adhikari[2]
[1, 2]*Department of Computer Science and Engineering, Tulsiram Gaikwad Patil College of Engineering, RTMNU, Nagpur, Maharashtra*

Abstract: ***Nowadays multimedia system knowledge protection is changing into important. The coding technique is employed to safeguard multimedia system knowledge. There are completely different techniques wont to defend confidential image knowledge from unauthorized access. during this paper, we've got an inclination to survey existing work that's used entirely completely different techniques for image coding and that we to boot give a general introduction relating to cryptography.***
Keywords: Encryption, Decryption, Data Encryption Standard (DES), Advanced Encryption Standard(AES), Blowfish, Modified Advanced Encryption Standard(MAES),Rubik's Cube Algorithm

I. INTRODUCTION

With the ever-increasing growth of multimedia system applications, a crucial issue for communication and storage of pictures is security, and coding is one in every of the techniques to make sure security. coding techniques convert the first image to a different image that's onerous to understand; to stay the image confidential between users, in different words, it's essential that no one might get to understand the confidential message while not a key for secret writing. Their completely different coding techniques are wont to shield confidential messages from unauthorized users. coding could be a quite common technique for promoting info security. The evolution of coding is moving towards a way forward for endless potentialities.

II. LITERATURE SURVEY

Some of the ideas utilized in cryptography square measure delineated here [1,2]:

A. Cryptography

1) *Plain Text:* Any communication within the language that we have a tendency to speak- that's the human language, takes the shape of plain text. it's understood by the sender, the recipient associated additionally by anyone UN agency gets an access to it message.
2) *Cipher Text:* Cipher means a code or a secret Message. once a comprehensible text is statute victimisation any appropriate theme the ensuing message is named as Cipher text.
3) *Secret Writing:* the method of changing of plain text Messages into cipher text messages area unit referred to as Encryption.
4) *Decryption:* The reverse method of secret writing i.e. Cipher text messages back to plain text is named as cryptography.
5) *Key:* A crucial component of playacting secret writing and cryptography is that the key. it's the key used for secret writing and cryptography that produces the method of Cryptography secure.

B. Purpose of Cryptography

1) *Authentication:* Authentication mechanisms facilitate to see proof of identities. This technique ensures that the origin of the message is correctly far-famed.
2) *Integrity:* The integrity mechanism ensures that the contents of the message keep equivalent once it reaches the meant recipient as sent by the sender.

C. Types of Cryptography

Two types of cryptography:

1) *Symmetric Key Cryptography:* When a similar key is used for both encryption and decryption, then that Mechanism is known as symmetric-key cryptography.
2) *Asymmetric Key Cryptography:* When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known as asymmetric key cryptography.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

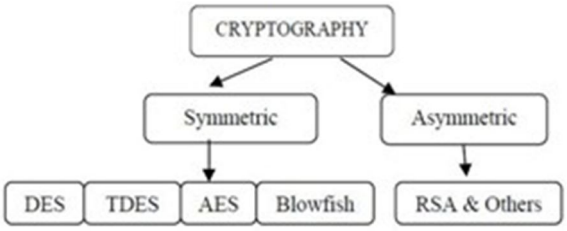


Figure1: Classification of Cryptograph

D. Data Encryption Standard (DES)

DES could be a block cipher that uses a shared secret key for encoding and cryptography. DES encoding technique is delineate by Davis R. [3] takes a fixed-length string of plaintext bits and transforms it through a series of difficult operations into cypher text bit string of constant length. within the case of DES, every block size is sixty four bits. DES uses a key of fifty-six bits for encoding so the cryptography method will solely be performed by those that understand the key that is employed for encrypting the message. There area unit sixteen stages of processing all stages area unit identical, termed rounds. there's conjointly AN initial and final permutation, termed information processing and FP, that area unit inverses (IP "undoes" the action of FP and vice versa). The Broad level steps in DES area unit as follows [1]:

1) In the beginning, the 64-bit plain text message is handed over to AN Initial permutation (IP) operate.
2) The initial permutation is performed on plain text.
3) The informatics produces 2 halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4) Now, every LPT and RPT undergo sixteen rounds of the secret writing method.
5) In the tip, LPT and RPT ar rejoined and a final Permutation (FP) is performed on the combined block.
6) The results of this method produces 64-bit cypher text. Rounds: every of the sixteen stages, in turn, consists of the broad level steps and is shown in Figure two.

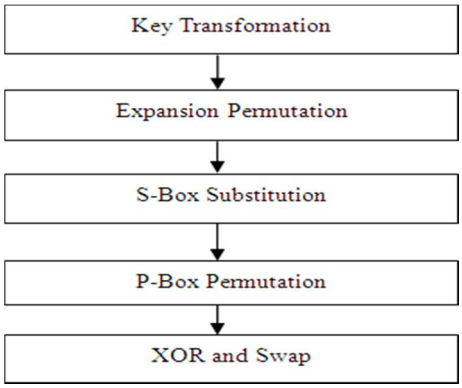


Figure2:DetailsofOneRound inDES

E. 3DES

3DES (Triple DES) is an Associate in Nursing improvement of DES; it's sixty four bit block size with 192 bits key size. during this normal the coding methodology is same as original DES however applied three times to extend the coding level and also the average safe time. it's a known proven fact that 3DES is take longer DES i.e. 3DES is slower than alternative block cipher strategies. It uses either 2 or 3 fifty six bit keys within the sequence Encrypt-Decrypt-Encrypt (EDE). Initially, 3 completely different keys square measure used for the coding algorithmic rule to come up with cipher text on plaintext message t,

C(t)=Ek1(Dk2 (Ek3(t)))…….(1)

Where C (t) is cypher text made from plain text t, Ek1 is that the secret writing technique victimisation key k1 Dk2 is that the cryptography technique victimisation key Dapsang Ek3 is that the secret writing technique victimisation key k3 an alternative choice is to use 2 completely different keys for the secret writing rule that reduces the memory demand of keys in TDES.

©IJRASET: All Rights are Reserved

C(t)=Ek1(Dk2(Ek3(t)))……..(2)

TDES formula with 3 keys needs i.e. 2^168 doable mixtures and with 2 keys needs 2^112 mixtures. it's much uphill to undertake such an enormous combination therefore TDES is the strongest encoding formula. The disadvantage of this formula it's too long consuming.

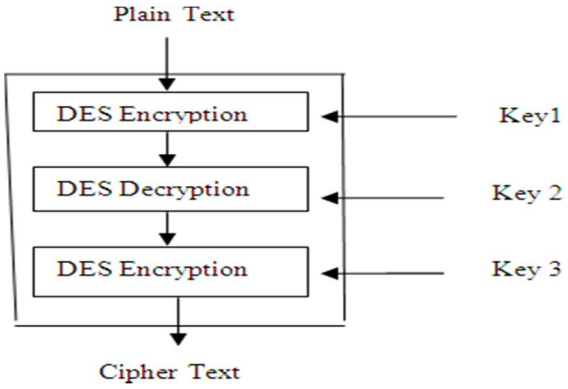


Figure3: 3DESalgorithm

F. Advanced Encryption Standard (AES)

The AES cipher [4] is nearly clone of the block cipher Rijndael cipher developed by 2 Belgian cryptographers, Joan Daemen and Vincent Rijmen. The AES algorithmic program may be a symmetric-key algorithmic program, which suggests a constant secret is used for each encrypting and decrypting the info. the quantity of internal rounds of the cipher may be a operate of the key length. the quantity of rounds for the 128-Bit secret is ten. in contrast to its forerunner DES, AES doesn't use a Feistel network. Feistel networks don't inscribe a complete block per iteration, e.g., in DES, 64/2 = thirty two bits square measure encrypted in one spherical. AES, on the opposite hand, encrypts all 128 bits in one iteration. This rounds.AES algorithmic program is shown in figure four.

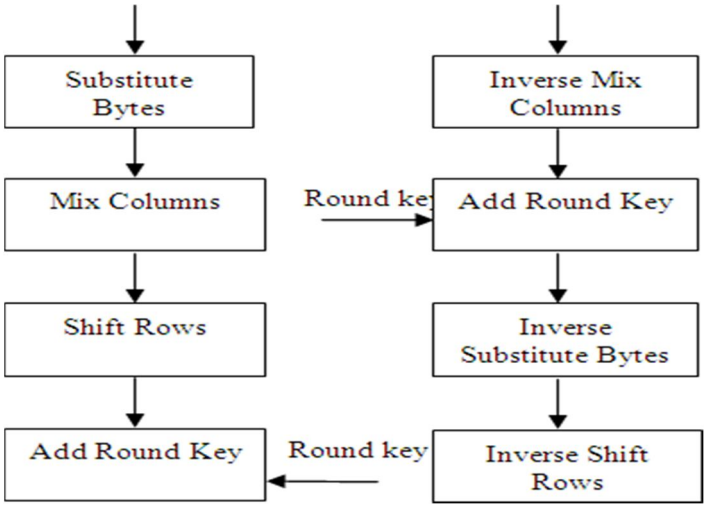


Figure4: One Round of encryption and Decryptionin AES

1) *Decryption:* Decryption involves reversing all the steps taken in secret writing victimization inverse functions like InvSubBytes, InvShiftRows, InvMixColumns. Encryption Round Decryption Round Each processing Roundinvolves foursteps:-
2) *Substitute Computer Storage Unit:* A non-linear substitution step wherever every computer storage unit is replaced with another computer memory unit using a hunt table.
3) *Shift Rows:* A transposition step throughout this step each row of the state is shifted cyclically a selected kind of steps.
4) *Mix Column:* In mixture operation, the columns of the state, combining the four bytes in each column.
5) *Add Spherical Key:* Each computer storage unit of the state is XOR With the roundkeyusingbitwise.

G. Blowfish

Blowfish [5] is one in every of the foremost common property right secret writing algorithms provided by Bruce Schneier. The blowfish secret writing is shown in figure5 below, Blowfish encrypts 64-bit block ciphers with variable lengths from thirty-two bits to 448 bits Key. It contains 2 elements

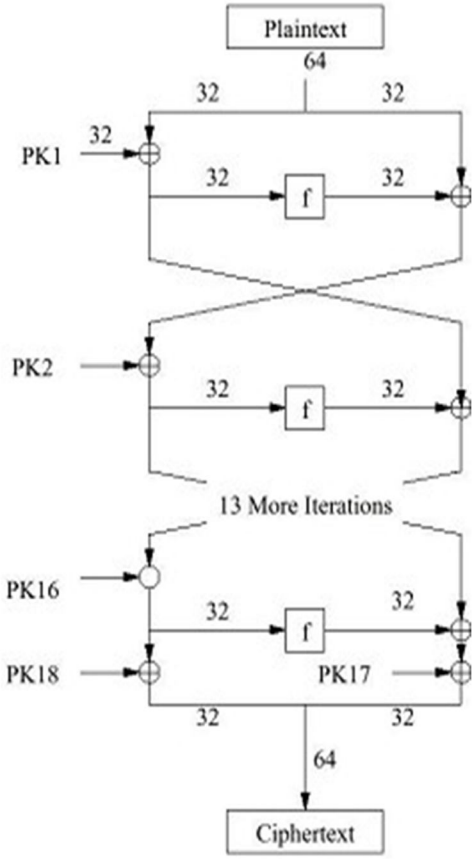


Figure 5:Blow fish Encryption

1) *Subkey Generation:* This method converts the key up to 448 bits long to subkeys to a complete of 4168 bits.
2) *Data Encryption:* during this half the iteration of a straightforward perform of sixteen rounds. every iteration contains a key-dependent permutation and key- and data-dependent substitution. Blowfish suits the applications wherever the key remains constant for an extended time (e.g. communication link encryption) however not wherever the key changes oftentimes (e.g. packet switching).

III. COMPARISON

Algorithm	*KeySize (Bits)*	*Block Size (Bits)*	*Average Encryption Time(Ms)*
DES	**56**	**64**	663.31
3DES	112 or 168	**64**	742.31
AES	256	**128**	542.38
BLOWFISH	32-448	**64**	91.92

Figure6:EncryptionTime of Each Algorithm (Inms)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

IV. METHODOLOGY

A. Modified Advanced Encryption Standard

The rule is split into four operational blocks wherever we have a tendency to observe the information at either bytes orbit levels and therefore the rule is intended to treat any combination of information and 128 bits of key size is versatile. The four stages that we have a tendency to use for Modified-AES rule are:

1) Substitution bytes
2) Mix columns
3) Shift Row
4) Add spherical Key

For secret writing, every spherical consists of the subsequent four steps:

a) Inverse shift rows
b) Inverse substitute byte
c) Add spherical ke
d) Inverse combine columns.

We try and modify the AES to be a a lot of economical and secure manner by adjusting the Shift Row part. Shift Row Phase: rather than the first Shift row, we have a tendency to modify it as:

- Check the worth within the initial row and initial Column,(state [0][0]) is even or odd.
- If it's odd, The Shift Rows step operates on the Rows of the state; it cyclically shifts the bytes in every row by a particular offset. For MAES, the primary And third rows ar unchanged and every computer memory unit of The second row is shifted one to the left. Similarly, the fourth row is shifted by 3 to the left severally.
- If it's even, The Shift Rows step operates on the Rows of the state; it cyclically shifts the bytes in every row by a particular offset. the primary and fourth Rows ar remains constant and every computer memory unit of the second row is shifted 3 to the correct. Similarly, the Third row is shifted by two severally on to the correct.

V. RUBIK'S CUBE PRINCIPLE AND PROCEDURE

The veritably conception of Rubik's cell depends on rows and columns. The principle is applied to rows and these rows rotated according to the demand. The image is divided into rows and each row pixel metamorphosis is applied.

Rubik's Cell Image Encryption In this section, the proposed encryption algorithm grounded on Rubik's cell principle is described along with the decryption algorithm.

Rubik's Cell Grounded Encryption Algorithm

Let Io represent a α- bit image of the size M ×N. Then, Io represents the pixels values matrix of image Io. The way of encryption algorithm are as follows

(1) Induce aimlessly two byte arrays BR and BK of variable length
(2) Store all the pixel values of a named image in a byte array BR
(3) Divide the byte array BR into three corridor and store it in three different byte arrays.
(a) The first byte array B1 will store pixel values from 0 to one-third part of BR
(b) The alternate byte array B2 will store pixel from the end of B1 till one-sixth of BR.
(c) The third byte array B3 will store remaining pixel from end of B2 till end of BR
(4) For each byte array i of image Io,
(a) Cipher the sum of all rudiments in the byte array i, the sum is denoted by α (i)

$$\alpha(i) = \sum_{j=1}^{N} Io\ i, j,\ i = 1, 2,., M, \quad (1)$$

(b) Cipher modulo2 of α (i), denoted by M α (i)
(C) Byte array i is left or right shifted depending on the M α (i)
If M α (i) = 0 right indirect shift
differently left indirect shift

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

(5) Using byte array BK, the bitwise XOR driver is applied to first and third byte array of the climbed image.
(6) Combine all the byte arrays B1, B2, B3 into another byte array Ienc in order to gain an translated image.
Rubik's cell decryption Algorithm.
The deciphered image is Idec is recovered from the translated image Ienc. The way for decryption algorithm is
(1) Divide the byte array Ienc into three corridor and store it in three different byte arrays.
(a) The first byte array B1 will store pixel values from 0 to one-third part of BR
(b) The alternate byte array B2 will store pixel one sixth part of BR
(c) The third byte array B3 will store remaining pixel values of BR
(2) Using byte array BK, the bitwise XOR driver is applied to first and third byte array of the climbed image.
(3) For each byte array i of image Io,
(a) Cipher the sum of all rudiments in the byte array i, the sum is denoted by α (i) N

$$\alpha(i) = \sum_{j=1} Io\ i, j\ , i = 1, 2, \ldots , M, \quad (1)$$

(b) Compute modulo2 of α (i), denoted by M α (i)
(c) Byte array i is left or right shifted depending on the M α (i)
If M α (i) =0 right circular shift
else left circular shift
(4) Combine all the byte arrays B1, B2, B3 into another byte array Idec in order to obtain an original image.

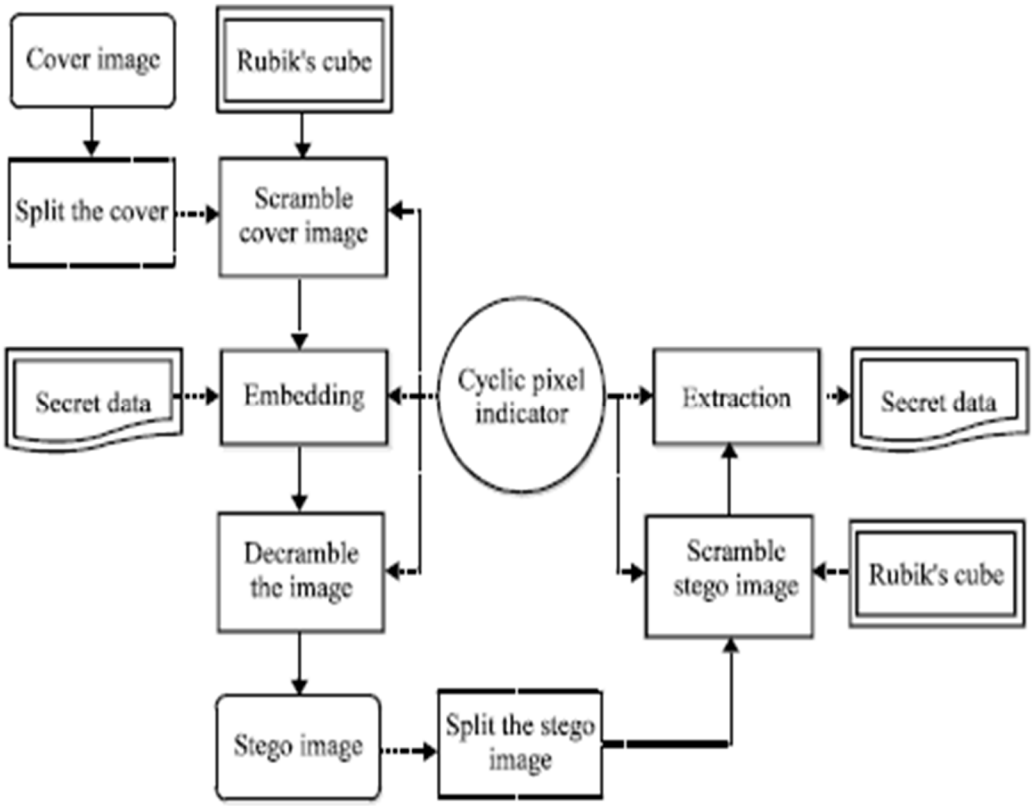


Fig: system flow Diagram

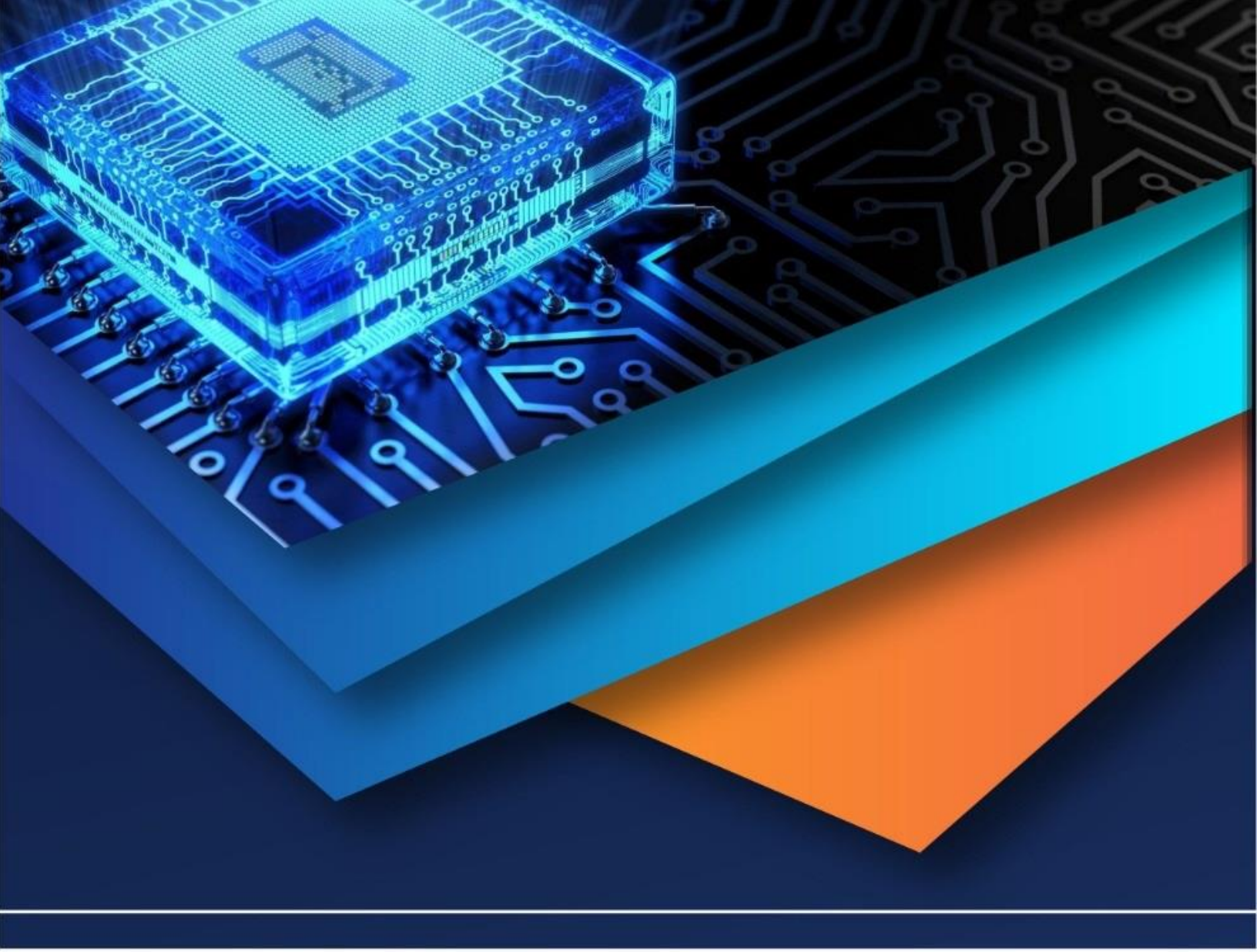
VI. CONCLUSION

This paper explains the encrypting and decrypting techniques. Rubik cube rule performance assessment tests demonstrate that the planned image coding rule is extremely secure. it's conjointly capable of quick coding/decryption that is appropriate for time period net encryption and transmission applications. The before mentioned algorithms ar economical and are repeatedly tested for concrete results, but, the moral facet of the answer should not be forgotten. The techniques mentioned higher than have to be compelled to be enforced ethically to provide desired results while not breaching any established security protocols.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] William Stallings "Network SecurityEssentials(Applications and Standards)", Pearson Education, 2004.
[2] BruceSchneier"AppliedCryptography,SecondEdition,JohnWiley&Sons1996.
[3] Davis,R.,"TheDataEncryptionStandardinPerspective,"ProceedingofCommunicationSocietymagazine,IEEE,Volume16No6, pp. 5-6,Nov. 1978.
[4] Manoj. B, Manjula N Harihar , "Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology (IJEAT) ISSN:2249–8958,Volume-1,Issue-5,June2012.
[5] PratapChnadraMandal"SuperiorityofBlowfishAlgorithm,"InternationalJournalOfAdvancedResearchinComputersScienceandSoftwareEngineeringVol2Issue 9, September2012.
[6] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, AmitKumar Mishra, "Textand Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & TechnologyinComputerScience,May–June 2014
[7] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha "Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of ElectronicsandCommunicationTechnologyVolume2Issue3,September2011.
[8] E.Thambiraja,G.Ramesh,Dr.R.Umarani,"Asurveyonvariousmostcommonencryptiontechniques,"InternationalJournalofAdvancedResearchinComputerScience andSoftwareEngineering,Vol2,Issue7,July2012.
[9] MonikaAgrawal,PradeepMishra,"AComparativeSurveyonSymmetricKeyEncryptionTechniques,"InternationalJournalonComputerScienceandEngineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.
[10] Salma Hesham, Mohamed A. Abd El Ghany and KlausHofmann,"HighThroughputArchitecturefortheAdvancedEncryptionStandardAlgorithm"IEEE2014.
[11] Pravin Kawle, Avinash Hiwase, Gautam Bagde, EkantTekam,RahulKalbande,"ModifiedAdvancedEncryptionStandard",InternationalJournalofSoftComputing and Engineering (IJSCE), Volume-4, Issue-1, March 2014.
[12] Sruthi B. Asok , P. Karthigaikumar, Sandhya R, NaveenJarold K, N.M Siva Mangai,"A Secure CryptographicScheme ForAudio Signals"IEEE2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)