International Journal of Advanced Technology and Engineering Exploration
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
Volume-2 Issue-13 December-2015

An efficient Image Security mechanism based on Advanced Encryption Standard

Priyank Singhai[1*] and Amit Shrivastava[2]
Mtech Scholar Department of computer science, Sagar Institute of Research & Technology , Bhopal, India[1]
HOD Department of computer science, Sagar Institute of Research & Technology , Bhopal, India[2]

Abstract

This paper presents an efficient scheme for image data encryption. In this paper an efficient framework has been presented for data security. In this framework two separate frames are designed separately for sender and receiver. In this paper an efficient Advanced Encryption Standard (AES) based algorithm has been proposed. In this process the Image data is selected first and then it is converted in the encrypted supported file that is a binary file. This data is the plaintext for the next processing. Then AES algorithm is applied for data encryption process. The key that is given as data is ventured into a cluster of 44 words (32-bits each), w[i]. 4 distinct words (128 bits) serve as a round key for each round. Then data substitution is applied. Then value is calculated according to the finite field that is Galois field. Then XOR is applied to the added round key. Then key randomization based Image conversion is applied with the help of proposed algorithm. So search key is needed based on the generated image.

Keywords

Image encryption, AES, XOR, Galois field.

1. Introduction

In the current scenario we see that the use of a single stage data encryption algorithm is not very secure. To overcome this situation a combined encryption algorithm is proposed in this paper. That is, the algorithm security is greatly enhanced, through researching several well-known data encryption algorithms, and improving some data encryption algorithms and arranging encryption algorithms in some sort of order.

*Author for correspondence

An improved concept is proposed by analysing the principle of the cryptography technique based on the combination of symmetric key and translation of plain text into an image. Moreover, the safety measures, security and performance of the proposed concept will also estimate [1]. The experimental results depend upon combination of symmetric and conversion of plain text into an image and finally attaching key will endorse the effectiveness of the proposed concept. The resultant cipher text which is generated by this method will be unreadable as well as perplexing that the information transferred is text or image and will be appropriate for realistic use in the secure transmission of confidential information over the Internet [2].

Disregard cryptography is mindful here the confederation of keyed equivalent and ability in pretending to pay deception walk are including beneficial than those developed utilizing unadulterated" proportional or uneven systems alone [1]. Standard in the fundamental, this takes the vicinity of a deviated cryptosystem the world suitably of a non-specific keyed mirror-like cryptosystem with certain bolster properties as a sub-schedule. This empowers the plan of tricky in which a few of the computational inconvenience is hypothetical by the about productive in extent cryptosystems undiplomatic trading off the field of the general cryptosystem [2][12][13]. Generally, disregard cryptography is rummage to Rather initiate encryption information at the obvious encryption of the correspondence is given by a consistent encryption plot want under an arbitrarily produced symmetric key [3][4][5]. The uneven encryption wish is problematically second-hand to encode this arbitrarily produced symmetric key. This permits the encryption objective to squire sting messages, an obligation with some immaculate unbalanced encryption plans [6][7].

Contemporaneous cryptosystem gives the power to content stabilizer for recommend in point of interest transmitting it absence of restriction an unreliable

channel [8]. The encryption plan is likewise recommended in [9]. Straightforwardly proof is transmitted over the web we get sanctuary letter, retreat, legitimacy and non-denial for it. In senior age encryption and computerized marks are concentrated on a significant obligation in end report privacy and information respectability yet autonomously [10]. Generally the report is rummage to stages saucy premise computerized seal and slanted the message is not publishable to convey to an end both the secrecy and information trustworthiness [11]. The craving is over and over flaunted as signature then encryption longs. The plan having pair pressurize: Shoddy adequacy and high cost of such recreation [12]. There is several other image encryption techniques are also discussed in [13-17]. Some related standard encryption techniques are also suggested in [18-21]. The main objectives are to solve the key exchange dilemma, transfers single file together with data as well as key and to improve the conventional cryptographic algorithm and make it effective against brute force attack.

2. Related Work

In 2011, Matalgah et al. [22] motivated by system coding hypothesis a productive half and half encryption-coding calculation that obliges utilizing customary encryption just for the first little measure of information. This measure of information, which we allude to as the first square, is controlled by the conventional encryption calculation to be connected on this first piece. In their proposed calculation, all whatever remains of the data will then be transmitted safely over the remote channel, utilizing system coding, without a requirement for utilizing customary encryption. The same with the distinctive methodology has been proposed in [23][24] .

In 2011, Wai Zin et al. [25] watch that because of expanding the advancements security frameworks are extremely well known in numerous territories. The security of data can be attained to by utilizing encryption and steganography. In cryptography, scrambled information is transmitted in the wake of changing the other frame rather than the first information. Contrast cryptography, data concealing procedure can be reached out for shielding from the intriguing of any assailant. They proposes the improve security framework by consolidating these two procedures. Their proposed framework means for information privacy, information validation and information trustworthiness. In 2011, Sandeep Bhowmik et al. [26] recommend that the adequacy of the insurance through encryption relies on upon the calculation connected and in addition on the nature of the "key" utilized. On the off chance that a "key" is severely outlined or erratically chose, clearly the assurance neglects to give fitting security and dishonorable access can be picked up on the secured data. The principal calculation in cryptographic framework outline is the calculation to create 'key'. It determines the way in which the "key" is to be picked. This work concentrates on an absolutely new approach towards the "key" era for encryption algorithms.

In 2011, Rohollah Karimi et al. [27] explore shortcomings in existing Geoencryption frameworks and propose a few answers for increment the wellbeing and dependability in these frameworks. For this reason they show another geoencryption convention that will permit portable hubs to impart to one another securely by confine disentangling a message in the particular area and time period. In 2012, Rajavel, D. et al. [28] proposed another cryptographic calculation in light of mix of hybridization and revolution of shapes. Hybridization was performed utilizing enchantment 3D shapes with m number of n request enchantment square for the creating crossover blocks. The got half breed solid shape was rearranged by means of pivot square, which thus created from haphazardly chose enchantment square. Cubic revolution was executed as same that of basic Rubik's shape rearranging.

In 2012, P. Fanfara et al. [29] recommend that Communication security is one of numerous informatics parts which have gigantic advancement. Delicate information is progressively utilized as a part of correspondence and that is the motivation behind why security prerequisite is all the more convenient and essential. The danger of getting information through different increments with upgrading the force of today's PCs. Their consideration is fundamentally given to sender validation in light of utilizing advanced signature and hilter kilter encryption by means of restricted hash capacity to figure open and private keys. In 2012, Lili Yu et al. [30] recommend that calculation security is extraordinarily enhanced, through examining a few renowned information encryption calculations, and enhancing some information encryption calculations, and organizing encryption calculations in some

request. At long last, the joined encryption calculation is effectively made by utilizing the starting encryption calculation, Micro Genard encryption calculation and the renowned Base64 encryption calculation. That is, as per the request of the starting encryption calculation, the enhanced Micro Genard encryption calculation and the well-known Base64 encryption calculation, the client's data is bit by bit scrambled, and the calculation security is significantly improved. In 2012, Seung-Hoon Cho et al. [31] proposes an ongoing information stockpiling framework that is made out of the pressure of the flight and voice information in view of DPCM, the encryption of the compacted information utilizing AES encryption calculation and the re-plan of the encoded information by rearranging system. The proposed framework is executed in equipment utilizing Verilog HDL and we tried the execution of the framework with the reproduction flight and voice information. Therefore, they found that the proposed framework pack the information proficiently and improves security qualities.

3. Proposed Work

The raw images are selected first in our approach. At that point we change over the picture in twofold measurement whole number exhibit through java. If it is support the conversion then we will process it for AES encryption. By AES encryption we will convert the original image in the encrypted form by changing and randomizing the pixel. Then XOR process will be applied and convert the AES + XOR form of the image. The process and the workflow are better understood from figure 1. Our encryption method is consisting of Advanced Encryption Standard (AES) encryption which generates the key along with the K random key generated. Then it will be send to the client.. Then the same key in the reverse order is needed when the client want to achieve this data. In the case of AES only one key is required. So it is must to adhere the accuracy on the all steps of the key arrangement and assignment so that the authorize client can access the data within the time frame without any delay. But it improves the security also because of the robust mechanism used by this framework.Our encryption method is consisting of Advanced Encryption Standard (AES) encryption which generates the key along with the K random key generated. Then it will be send to the client. Then the same key in the reverse order is needed when the client want to achieve this data. In the case of AES only one key is required. So it is must to adhere the accuracy on the all steps of the key arrangement and assignment so that the authorize client can access the data within the time frame without any delay. But it improves the security also because of the robust mechanism used by this framework.

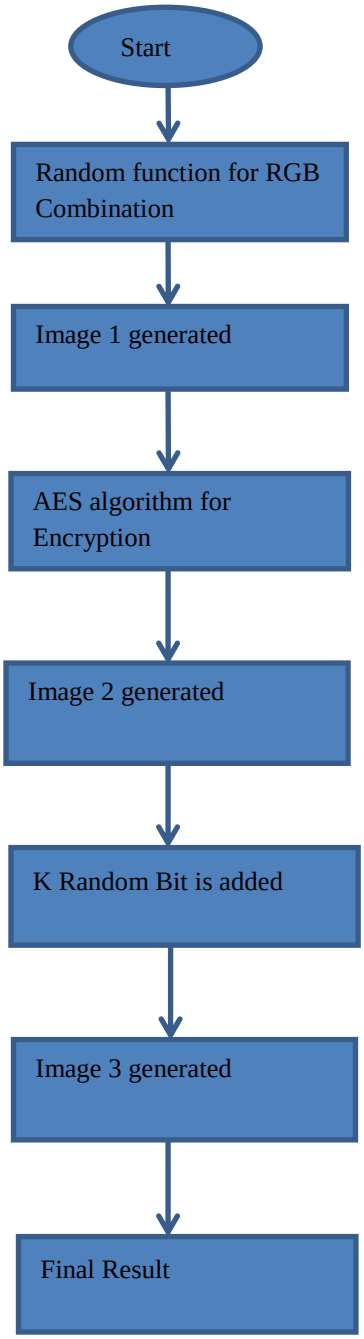

Figure 1: Flowchart

Then AES algorithm is applied for data encryption process. In this process the plain text is applied to AES algorithm. The key that is given as data is ventured into a cluster of 44 words (32-bits each), w[i]. 4 distinct words (128 bits) serve as a round key for each round. Then data substitution is applied. Then value is calculated according to the finite field that is Galois field. Then XOR is applied to the added round key. Then key randomization based Image conversion is applied with the help of the below algorithm.

Algorithm

Step 1: A random number between 1 to N is generated for applying with the RGB combinations.
Step 2: Image 1 is generated based on the RGB values generated based on the N values.
Step 3: Regenerate a new random number between 1 to K.
Step 4: K is the search key for the database.
Step 5: The image is then encrypted with the AES algorithm. Image 2 is generated based on algorithm 1.
Step 6: Image 3 is generated based on the K pixel of RGB values.
Step 7: Image 3 is ready to send to the receiver.
Step 8: Receiver receives it.
Step 9: The K value attached is removed to get Image 2.
Step 10: The K value provides the hint for the decryption key in the search space.
Step 11: Image 2 is decrypted using AES key.
Step 12: Generate Image 1 by reading the last N value. Data transformation is applied to retrieve it.

This paper has been developed to improve the algorithm which was proposed by the Ahmad Abusukhon and Mohammad Talib [1]. The main drawback of their algorithm is that it does not solve the key exchange problem. Another disadvantage is that they are transferring the whole key value. This is very big in size (key1) as each character in plain text is replaced by three random numbers. Another drawback is that they are also including # as a delimiter Therefore it requires transferring at least six times more data as compared to actual data for decrypting the packet. Further they have also not described the actual key exchange method of key1 and key2; in key2 they have only just swapped the column of the generated matrix which is not very secure method as compared to AES encryption. As we know encryption is more secure method as compared to swap operations so the proposed technique executes an encryption stage rather shuffling the positions of bits by matrix scrambling technique. The sender & receiver side has a combination database which contains number of combinations of text to digits mapping. It has various combinations of transforming characters into equivalent RGB values. The character is transformed into an RGB pixel where total intensity of the pixel depends upon the intensities of Red Green and Blue colour values at that position also each combination have assigned a unique number which ranges from 1 to N. N denotes the total number of combinations in the database. The process starts from the sender side. In this research we have taken N as 10. The sender generates a random number between 1 to 10. This represents the combination number to be applied for transformation of Text to an Image. Using the corresponding combination (key1) transformation method proposed in [1] is applied which results in the generation of an image. Hence we see that the text is totally converted into an image. The number N is attached in the image by adding one more pixel in the image at last. We have attached one more pixel which is having Green and Blue component of zero intensity value, the Red component of this pixel will store the number N and finally this will result in the formation of Image1. Now sender generates a random number between 1 to K. Here we have taken K as 10. Sender Matches the corresponding key (Key2) in Key database. This key2 is used for AES Encryption. Now the image generated by Text to image transformation is encrypted by key using an AES algorithm [13].

The number K is finally attached in the image by adding one more pixel in the image at last with the same method as was applied to attach N. Finally this single file is transferred to the Receiver. When Receiver receives the final image, the first task is to read the last pixel to get the combination number. When this number is obtained the number is matched in the Key database which retrieves the corresponding key (key2). Now the last pixel is discarded from the image and the resultant image is decrypted using key2 and AES algorithm. Now Receiver reads the last pixel to get the combination number. When this number is obtained the number is matched in the combination database which retrieves the corresponding key. (key1). Now the last pixel is discarded from the image. Finally key1 is applied on

the generated image which transforms image into original plain text.

4. Result Analysis

We have built the sender's and Receiver's programs on different machines and use the following text message for our experiments: "encryption is the process of converting data to a form called a cipher text which cannot be easily understood by unauthorized people decryption is the reverse process for converting encrypted data back to its original form so that it can be understood. The use of encryption decryption method is old but strong art of communication in wartime. Cipher is often incorrectly called a code which can be employed to keep the enemy away from obtaining the contents of transmissions". The data is of the size 1137 bytes, we have taken first 200,400,600,800 and 1000 bytes of data for analysis.

Table 1: Encryption and Decryption time calculated

Text Size (Bytes)	Encryption Time (Sec)	Decryption Time (Sec)
200	1	1
400	2	2
600	4	3
800	5	4
1000	6	5

From table 1 we can easily see that encryption time is increasing 1 second per 200 bytes of data as we see that for 200 bytes of data the encryption time obtained is 1 second, for 400 bytes of data the encryption time obtained is 2 seconds, for 300 bytes of data the encryption time obtained is 3 seconds and so on. The decryption time is less than the encryption time, the reason what we see for this is that we are doing maximum write operations in encryption phase while the decryption phase contains maximum of the read operations.

For analysing the results graphically we have taken size of the text at X-axis of a two dimensional plane and time is taken at Y-axis Figure-2. We have plotted two graphs one for encryption and another for decryption. Plotting the graph of the results obtained from the Table 1 we observed a straight line for encryption phenomena which is nearly 45 degree from the origin, we also see that the decryption time is not same as encryption time and its graph is not increasing with a constant slope with respect to increase in data. But it is clear from the graph that with the increase in size of the data blocks both the Graphs weather it is related to encryption and decryption its time is increasing directly proportional to the increase in the size of the data.

The existing technology is also having one drawback as it is transferring whole key every time whenever the transmission of the data takes place. This key is quite big in size [1].

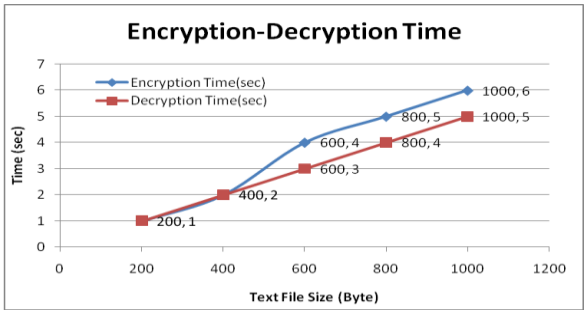

Figure 2: Graphical Analysis for Experimental Results

They have used three characters for substituting each character into pixel. Figure 3 compares the space complexity of the existing and proposed technique. In the existing method the developers have transferred the whole data definition for transferring every alphabet hence they need additionally they have used # as a delimiter to separate the text hence 3 extra # is used which results into total 6 extra characters per alphabet, hence they need a total of 26*6=156 characters extra. In JAVA every character takes 2 bytes of memory space and hence 156 characters will take 156*2=312bytes or which is equal to 312*8=2496 bits. Similarly if the existing technology takes digits also in account for RGB substitution it will result into 36 characters and the extra bits required for the decryption of such data will be 36*6*2*8=3456 bits. Similarly if the existing technology takes digits and special characters also in account for RGB substitution it will result into 69 characters and the extra bits required for the decryption of such data will be 69*6*2*8=6624 bits. Similarly if the existing technology takes digits, special character and case sensitivity of the characters also in account for RGB substitution it will result into 95 characters and the extra bits required for the

decryption of such data will be 36*6*2*8=9120 bits. While if we talk about the proposed technique it always need 2 integers one for Combination database for RGB and one for Combination database of key and auto matically generate keys at the receiver side. In JAVA 2 integers will take 4 bytes of space each hence 2 integers will take 8 bytes of memory space which is equal to 64 bit of extra data for decrypting cipher text at the receiver end.

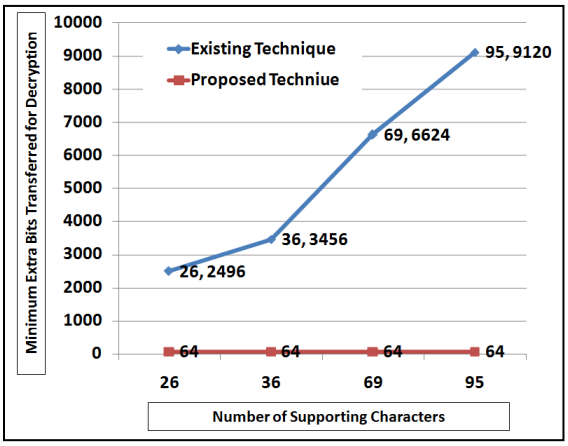

Figure 3: Space complexity between Existing and Proposed Technology

The best outcome is that only a single file is being transferred which in itself contains key, The Encryption time includes time taken in attachment of key and similarly Decryption time also includes the fetching of key from the cipher. The approach used in [1] only undergoes transformation of only 26 characters. We have used 95 character set including special characters of the keyboard. With the simple calculation, the number of possible Permutations to encrypt 95 letters is ((256) 3)95. Since each pixel is made by the combination of three values (RGB) and each one of these values ranges from 0 to 255, choosing three values has (256) 3 permutations.

Table 2: Comparison Table for Existing and Proposed Technology

Feature	Existing	Proposed
Key Exchange	No method implemented	Implemented Combination Database
Extra Private Channel Required for Key Transmission	Yes	No
Minimum Data transfers	2	1
Supporting Characters	26	95
Minimum Extra Bits Transferred for Decryption	2496	64
Minimum number of calculations for Brute force attack	$((256)^{3)926}$	$((256)^{3)95}$

We have 95 letters and thus the permutations for 95 letters is ((256)3)95 which is equal to 2.230437785918792147855758532010 5e686. Our approach also uses AES encryption stage hence one need 2128 different numbers of combination to break the cipher. Hence we can say that our approach is highly secure.

5. Conclusion

An efficient technique has been proposed in this paper for developing a highly secure transmission of text. If an intruder any how decrypts the image then he gets another image which is also in an unreadable form, this further confuses him that whether the actual information is in text or in image format, the blend of transformation of a text into an image and then encrypting the result with AES encryption makes actual information (plain text) highly secure for transmitting it on extremely vulnerable and highly insecure network environment.

The key which is needed to decrypt the text is sent with the image file and take only 64 bits extra space for any amount of data hence this work does not need any private or secure channel for key exchange, The Research work proposed sends only a single file for both data and key hence uses the communication channel only ones.

References

[1] Ahmad Abusukhon and Mohammad Talib, "A novel network security algorithm based on private key encryption" IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 2012, pp. 33-37.

[2] M. Kiran Kumar, S. Mukthyar Azam, and S. Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique", International Journal of Network Security and its Applications, 2010, pp. 30-41.

[3] Komal D Patel, Sonal Belani "Image Encryption using different Techniques" International Journal

of Emerging Technology and Advanced Engineering Volume: 1, Issue: 1, 2011, pp. 30-34.

[4] P.Karthigaikumar Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on Computational Science - New Dimensions & Perspectives", 2011.pp. 166-172.

[5] Manoj.B, Manula N Harihar "Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology, Volume: 1, Issue: 5, June 2012.pp. 290-294.

[6] Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security Volume: 12, Number: 04, pp. 18-31.

[7] P. Radhadevi, P. Kalpana "Secure Image Encryption Using AES" International Journal of Research in Engineering and Technology Volume: 1 Issue: 2, pp. 115-117.

[8] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm" International Journal of Computer Science Issues Volume: 9, Issue: 4, 2012, pp. 51-57.

[9] Praveen.H.L , H.S Jayaramu, M.Z.Kurian "Satellite Image Encryption Using AES" International Journal of Computer Science and Electrical Engineering (IJCSEE), Volume:1, Issue: 2, 2012, pp. 56-60.

[10] Whitfield Diffie, "The First Ten Years of Public Key Cryptography", Proceedings of the IEEE Volume 76, 1988 pp. 560-577.

[11] W.E. Burr, "IEEE Security and Privacy Volume: 1, Issue: 2", 2003, pp. 43-52.

[12] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal Volume: 6, Issue: 2, 2010, pp. 1-14.

[13] Nazmudeen, Naida H., and F. J. Farsana. "Satellite Image Security Improvement by Combining DWT-DCT Watermarking and AES Encryption." International Journal of Advanced Computer Research 4, no. 2 (2014): 645.

[14] Sandhya Rani M.H., K.L. Sudha, "Design and Implementation of Image Encryption Algorithm Using Chaos", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.660-664.

[15] Arunabha Sengupta, "Dynamic fragmentation and query translation based security framework for distributed databases", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-20, September-2015, pp.249-263.

[16] Ketki P. Kshirsagar, " Key Frame Selection for One-Two Hand Gesture Recognition with HMM " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015 ,pp.192-197.

[17] Nanda Hanamant Khanapur and Arun Patro, " Design and Implementation of Enhanced version of MRC6 algorithm for data security " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015 ,pp.225-232.

[18] Dubey, A.K., Dubey, A.K., Namdev, M. and Shrivastava, S.S., 2012, September. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In Software Engineering (CONSEG), 2012 CSI Sixth International Conference on (pp. 1-8). IEEE.

[19] Manju Kaushik, Gazal Ojha , " Attack Penetration System for SQL Injection " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.724-732.

[20] Urmi Chhajed, Ajay Kumar, "Detecting Cross-Site Scripting Vulnerability and performance comparison using C-Time and E-Time", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.733-740.

[21] Bhavesh Joshi and Anil Khandelwal, "Rivest Cipher based Data Encryption and Clustering in Wireless Communication", International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-2, January-2015, pp.17-24.

[22] Matalgah, Mustafa M. ,Magableh, A.M., "Simple encryption algorithm with improved performance in wireless communications",IEEE 2011.

[23] Asoke Nath, Debdeep Basu, Surajit Bhowmik, Ankita Bose, Saptarshi Chatterjee, " Multi Way Feedback Encryption Standard Ver-2(MWFES-2) " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-13, December-2013 ,pp.28-34.

[24] Sagar Chouksey, Rashi Agrawal, Dushyant Verma,Tarun Metta, " Data Authentication Using Cryptography " , International Journal of Advanced Computer Research (IJACR), Volume-3, Issue-10, June-2013 ,pp.183-186.

[25] Wai Wai Zin and Than Naing Soe ," Implementation and Analysis of Three Steganographic Approaches", IEEE 2011.

[26] Sandeep Bhowmik and Sriyankar Acharyya," Image Cryptography: The Genetic Algorithm Approach",IEEE 2011.

[27] Rohollah Karimi and Mohammad Kalantari, "Enhancing security and confidentiality in

location-based data encryption algorithms", IEEE 2011.

[28] Rajavel, D., Shantharajah, S.P., "Cubical key generation and encryption algorithm based on hybrid cube's rotation",IEEE 2012.

[29] P. Fanfara, E. Danková and M. Dufala, "Usage of Asymmetric Encryption Algorithms to Enhance the Security of Sensitive Data in Secure Communication", 10th IEEE Jubilee International Symposium on Applied Machine Intelligence and Informatics, SAMI 2012.

[30] Lili Yu, Zhijuan Wang and Weifeng Wang, "The Application of Hybrid Encryption Algorithm in Software Security", 2012 Fourth International Conference on Computational Intelligence and Communication Networks.

[31] Seung-Hoon Cho, Chan-Bok Jeong, Seok-Wun Ha, Yong Ho Moon," A Flight Data Storage System with Efficient Compression and Enhanced Security", IEEE 2012.