Survey on Different Image Encryption TechniquesWith Tabular Form

Pooja Hardiya[1] Ravindra Gupta[2]
[1]M.Tech. Student [2]Associate Professor
[1,2]Department of Computer Science & Engineering
[1,2]R.K.D.F. Institute of Science & Technology, Bhopal, Madhya Pradesh, India

Abstract— Rapid growth of digital communication and multimedia application increases the need of security and it becomes an important issue of communication and storage of multimedia. Image Encryption is one of the techniques that are used to ensure high security. Various fields such as medical science military in which image encryption can be used. Recent cryptography provides necessary techniques for securing information and protective multimedia data. In last some years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from illegal way in. Within this paper survey of different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used.

Keywords*:* Information Security, Image Encryption, DES, AES, Cryptography

I. INTRODUCTION

Due to some inherent feature of image like low cost and high availability, usage of communication network has increased and it becomes a reason for rapid growth of the internet in the digital world today. In our society digital images play a more significant role than the traditional texts and it need serious protection of user's privacy for all applications. So the security of digital images has become more important and attracted much attention. The security of digital image can be achieved by digital image encryption technique. Basically Image Encryption means that convert the image into unreadable format so that third party cannot interpret them. Various digital services need reliable security in storage and communication of digital images [1].

To prevent image from unauthorized access, Encryption techniques of digital images play a very important role .Since Digital images are exchanged over various types of networks and a large part of this digital information is either confidential or private. So Encryption is the preferred technique for protecting the transmitting information. There are various encryption systems to encrypt and decrypt image data. But, it can be said that there is no single encryption algorithm which satisfies the different image types [2].

In general, most of the available traditional encryption algorithms are used for text data. Although we can use the traditional encryption algorithm to encrypt images directly, this may not be a good idea for some reasons. First, image data have their special features such as high redundancy, and high correlation among pixels. Second, they are usually huge in size that makes traditional encryption methods difficult to apply and slow to process. third, the decrypted text must be equal to the original text but this requirement is not necessary for image data because characteristic of human insight, a decrypted image containing small distortion is usually acceptable .So the algorithms that are good for textual data may not be suitable for multimedia data, Even though triple data encryption standard (T-DES) and international data encryption algorithm (IDEA) can achieve high security, they may not be suitable for multimedia applications Therefore, well known encryption algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Standard (IDEA) were built for textual data not for multimedia data [3-4].

There are many types of image encryption methods. The image encryption algorithms can be categories into three major groups [5].

- Position Permutation (Transposition) Based Algorithm.
- Value Transformation (Substitution) Based Algorithm.
- Position- Substitution Based Algorithm

In a Position Permutation (Transposition) Based Algorithm elements are rearranged in the plain image. The rearrangement of element can be done by bit wise, pixel wise, or block wise. The permutation of bits decreases the perceptual information, but the permutation of pixels and blocks produce high level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8 (as the number of bits in each pixel).

Values Transformation Based algorithm is based on the technique in which the value of each pixel is change to some other value. The new value of pixel is evaluated by applying some algorithm on pixel .Basically algorithm is mathematical computation where we take input as a pixel value compute it, with some formulas and produce a new value for that pixel .

This technique is combination of both position permutation and value transformation. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values. The Position-Substitution Based Algorithm is use for the various techniques.

II. PERFORMANCE PARAMETERS

The performance of the encryption technique is measured by some of the basic parameters which are listed below: [6].

A. Visual Degradation (VD)

Visual degradation identifies the perceptual distortion of the image data with respect to the plain image.

B. Compression Friendliness (CF)

Compression Friendliness measures no or very little impact on data compression efficiency on the image . Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption.

C. Format Compliance (FC)

Format Compliance parameter is used to measures compliance the encrypted bit stream with the compressor. Standard decoder should be able to decode the encrypted bit stream without decryption.

D. Encryption Ratio (ER)

This measures the amount of data to be encrypted. Encryption ratio should be minimized so that the computational complexity can be reduced.

E. Speed (S)

This parameter measures how fast the encryption and decryption algorithms enough to meet real time requirements.

F. Cryptographic Security (CS):

Cryptographic security is used to identify whether encryption scheme is secure against different plaintext-cipher text attack.

III. Literature Review

Mohammad Ali Bani Younes and Aman Jantan 2008, [7] projected a block-based transformation rule supported the mix of image transformation and a standard secret writing and cryptography rule referred to as Blowfish. 1st of all the initial image was divided into blocks, before looking attention of secret writing method, these blocks square measure remodeled. At the receiver side these blocks square measure retransformed in to their original position and cryptography method is performed. Advantage of this approach, is that it reproduce the initial image with no loss of knowledge for the secret writing and cryptography method we have a tendency to use a blowfish rule. The results implies that once we inflated the quantity of blocks by exploitation smaller block sizes , shriveled correlation and inflated entropy.

Mohammad Ali Bani Younes and Aman Jantan 2008, [8] introduced a replacement permutation technique supported the mix of image permutation followed by secret writing I.e. standard secret writing rule referred to as RijnDael. Their projected technique work as follows: the initial image was divided into four pixels × four pixels blocks then the blocks were remodeled into new locations that were rearranged to create a permuted image employing a permutation method given, and so the generated image was encrypted exploitation the RijnDael rule. The correlation between image pixels was considerably shriveled, owing to arrangement of the blocks and so it becomes terribly troublesome to predict the worth of any given constituent from the values of its neighbors. What is more, this method of dividing and shuffling the positions of image blocks confuses the connection between the initial images and therefore the generated one .At the receiver, the initial image may be reproduced by the inverse permutation of the blocks.

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di 2009, [9] they all researches and work on the chaotic and DES encryption and also work a combination of image encryption algorithm. First of all they introduce a new encryption scheme by the use of logistic chaos sequencer to make the pseudo-random sequence, and also carries on the RGB with this sequence to the image chaotically, with the improvement of DES they makes double time encryptions. Their result represents higher starting value sensitivity, and high security and the high encryption speed.

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab 2010, [10] are proposed image encryption technique which is based on the two chaotic logistic maps and they are used an external secret key of 104 bit are employed to mystify the correlation between the cipher image and the plain image, and added the two chaotic logistic maps and to make the cipher more strong against any attack, after the encrypting of each pixel of the plain image the secret key is modified. The strength of the proposed system which makes the encryption of each plain pixel depends on the key is very secure and strong.

Amitava 2011, [11] Projected a 2 section secret writing and cryptography algorithms that's supported shuffling the image pixels exploitation affine rework and that they encrypting the ensuing image exploitation XOR operation in year 2011. With the assistance of 4 8-bit key applied, the constituent values square measure decentralized on completely different location exploitation affine rework technique. Within the next stage the remodeled image divided into two pixels x two pixels blocks and each block is encrypted exploitation XOR operation by exploitation four 8-bit keys. The key utilized in this rule is s sixty four bits long. Their results tested that when the affine rework the correlation between constituent values was considerably shriveled.

Yicong Chow and Sos Agaian 2011, [12] introduce a replacement methodology of applying the image steganography conception for image secret writing. They used the conception of e PLIP (Parameterized exponent Image Processing) addition to imbed the disorganized original image into a particular cowl image, it generates attention encrypted image. The parameterized exponent image process (PLIP) model may be a mathematical framework supported set of precise operations that may be applied to the process of intensity pictures valued in a very finite vary. Result analysis shows that the rule encompasses a terribly giant key area and may stand up to many common attacks.

Yun and Gunayi Wang 2011, [13] projected a changed chaotic map technique so as to boost the safety of chaotic secret writing rule. one in all the advantage of their technique is that once we compared it with original logistical map, their projected map makes it invariably be chaotic, and expands the iteration vary from original (0, 1) to (0, 4λ) (λ>0.25). This can be necessary for increasing key area of chaotic sequence and enhancing rate of amendment of chaotic signal. Attention secret writing rule is meant supported this chaotic map and a few analyses is given to indicate its sensible potency. Experimental results show that the changed logistical map possesses quicker secret writing, quicker sequence generation rate, larger key area and speed against the initial logistical map in 2011.

Zhang 2011, [14] projected a picture secret writing methodology supported total shuffling theme This methodology is characterized in this the key code stream utilized in secret writing isn't solely related to the key, however additionally associated with the plain image. as a result of the random range utilized in the diffusion method is obtained by iterating the skew tent map, and therefore the range of iterations is set by the previous constituent price of cipher image which incorporates the knowledge of previous constituent price of plain image, future random range is indirectly associated with the previous constituent price of plain image. This plain image connected secret writing methodology is powerfully against chosen plaintext attacks [27]. However, the primary cipher isn't safe enough to resist

the chosen plaintext attack, that is acknowledged and sepulcher analyzed in [28].

Qiudong 2012, [15] given a random scrambling rule supported bit-planes decomposition of image. Their rule starts by moldering a grey image into bit-plane pictures, every image for separate bit plane. Within the next step as plane image is shuffled by employing a random scrambling rule. At last, the entire shuffled bit plane pictures square measure integrated consistent with their original levels on bit-planes and that we obtained attention encrypted image. Experimental results show that the projected rule disorganized a picture effectively in addition as modified its bar chart apparently. it's higher potency and properties than the final random scrambling methodology. So it's additional stable scrambling degree than the classical methodology like Arnold rework.

Sukalyan and Atanu Kotal 2012, [16] given multiple chaotic maps primarily based a new regular image secret writing rule. Within the projected rule, with the assistance of generalized Arnold Cat Map, the plain image is 1st disorganized. Further, the disorganized image at a selected iteration is encrypted exploitation chaotic sequences generated by one-dimensional logistical Map when preprocessing them to integers. The results indicate that the projected rule will with success write and decode grayscale pictures with secret keys. It additionally exhibit that the projected methodology is secure, loss-less, and economical.

Shetty Deepesh Sadananda & Anusha Karkala 2013, [17] have represented a new methodology by using an image encryption technology which are based on two levels namely intensity variation and pixel color value swapping .Which performs the decryption operation in which the process are used as a reverse like after travels via network and reaches the intended receiver. For this decryption operation the secret keys are used to get back the original data without any risk of information leaked out to the third parties. The algorithms are used: - Two types of encryption methods have used Intensity variation in which three random numbers rb,gr,rr are used and in Pixel value Swapping in which input image is divided into 4 blocks b1,b2,b3 and b4.In this proposed methodology two levels of different securities are provided firstly the intensity variation and secondly pixel value Swapping.

Rintu Jose 2013, [18] A Separable Reversible Data Hiding in Encrypted Image with Improved Performance, proposes a novel scheme to reversibly hide data into encrypted grayscale image in a separable manner. During the first phase, the content owner encrypts the image by permuting the pixels using the encryption key. The data hider then hides some data into the encrypted image by histogram modification based data hiding, making use of data hiding key. At the receiver side, if the receiver has only encryption key, he can generate an image similar to the original one, but cannot read the hidden data. Peak Signal to Noise Ratio (PSNR) of this decrypted image is much higher than the existing methods. If the receiver has only data hiding key, he can extract the data, but cannot read the content of the image. If the receiver has both keys, he may first extract the data using data hiding key and then decrypt the image using encryption key. The method also has a higher data hiding capacity than the existing reversible data hiding techniques in encrypted image.

Nadiya P v, B Mohammed Imran 2013, [19] presented Image Steganography in DWT Domain using Double-stegging with RSA Encryption-The need for preserving secrecy of sensitive data has been ever-increasing with the new developments in digital communication. In this paper, we present an advanced method for embedding encrypted secret data in grayscale images to provide high level security of data for communication over unsecured channels. The proposed system combines the features of Cryptography and Steganography. Cryptography involves converting the secret message into a non-recognizable cipher. Steganography is then applied using Double-stegging to embed this encrypted data into a cover media and hides its existence.

A.Kester 2013, [20] projected a replacement technique that contribute to the final body of data within the space of cryptography application by developing a replacement cipher rule for image secret writing of m*n size by shuffling the RGB constituent values. With the assistance of RGB pixels, this rule ultimately encrypts and decrypts the photographs. The rule was enforced exploitation MATLAB. During this methodology, neither the bit values of the constituent square measure affected and nor constituent growth at the tip of the secret writing and therefore the cryptography method. Inside of the numerical values square measure backward, reshaped and concatenated with the RGB values, it shifted aloof from its various positions and therefore the RGB values interchanged so as to get the cipher image. This shows that, the full amendment within the total of all values within the image is zero. So there's no amendment within the total size of the image throughout secret writing and cryptography method. Advantage of their methodology is that the characteristic sizes of image can stay unchanged, whereas the secret writing method is being performed.

Eslami 2013, [21] used attention improved rule over these shortcomings delineated in [28]. 2 major enhancements, like exploitation previous cipher image pixels to execute "add modulus and xor" operations rather than plain image pixels, and enlarging the iteration times of chaotic system in each spherical, build the image secret writing theme projected in [26] higher security against the chosen plaintext attacks with slower secret writing speed as a trade off. Yong zhang [20] projected a search table primarily based secret writing improvement on the schemes projected in [12, 19] to boost the secret writing speed.

IV. Performance Comparison In Tabular Form

This section presents performance and comparison among image encryption schemes with respect to various parameters as shown in Table 1

Encryption Technique	Method used	Merits	Demerits
Encryption Image secret writing exploitation Block-Based	Original image is split into blocks, that square measure rearranged into a remodeled	No key generator, correlation between image parts shriveled	Image loosing and lower Correlation, no commonplace technique is

Transformation rule, 2008.	image employing a transformation rule given, and so the remodeled image was encrypted exploitation the Blowfish rule.	and better entropy.	employed for block transformation.
A Combination Of Permutation Technique Followed By secret writing, 2008.	1st pixels is shuffles supported permutation techniques used and so shuffled pixels is encrypted exploitation RijnDael rule.	Higher Entropy and Correlation between image elements decreased.	Permutation method is just too complex, Time taking and additionally chances of mistakes square measure high.
Image Encryption based on Chaos and Improved DES, 2009.	The logistic chaos sequence makes the Pseudorandom sequence and carries on the RGB with the sequence to the Image Chaotically, then make encryption with improved DES.	High Starting value sensitivity and high security and encryption speed.	Due to lots of mathematical computational, it takes long time to encrypt the image.
Image Encryption based on Composition of Two Chaotic Logistic Maps, 2010.	An external secret key of 104 bit are employed to mystify the correlation between the cipher image and the plain image, and added the two chaotic logistic maps.	Each plain pixel depends on the key is very secure and strong.	Lengthy, complicated, Time Consuming and chances of mistakes is high.
Image secret writing exploitation Affine Transform And XOR Operation, 2011.	Distribute the constituent values to completely different location exploitation affine rework technique remodeled image is then encrypted exploitation XOR operation.	Better resolution and Correlation between pixels values considerably decreases.	Lengthy, complicated, Time intense and Chances of mistakes are high.
Image secret writing exploitation the Image Steganography Concept and PLIP Model, 2011.	A modified chaotic map, which is based on the Logistic map, is used for image encryption to write to original image it's embedded into the dual image; it fuses the disorganized original image with the dual image exploitation the PLIP addition via specific parameters.	Giant key area will stand up to many common attacks.	Owing to uncountable mathematical process, it takes durable to encrypt the image; correlation between pixels still exists.
Image secret writing supported Bit-plane Decomposition and Random Scrambling,2012	Decomposes a grey image into many bit-plane pictures Then shuffles them by a random scrambling rule on an individual basis. Lastly, merges the disorganized bit-plane pictures consistent with their original levels on bit-planes attention gained an encrypted image.	Better potency, additional stable scrambling degree than the classical methodology, image bar chart is modified apparently.	Terribly time intense, Some style of security downside, secret's sensitive to crack. No specific technique is employed for scrambling.
Confusion and Diffusion of Grayscale footage exploitation Multiple Chaotic Maps, 2012.	The plain image is first scrambled exploitation generalized Arnold Cat Map. Further, the scrambled image at a particular iteration is encrypted exploitation chaotic sequences generated by one-dimensional supplying Map.	Loss-less, secure and economical, low correlation among pixels, a really big key house. High sensitivity to secret keys.	Time taking and risky, no changes in shuffled chart, quality of secret writing is low.

Encryption and cryptography of Digital Image victimization Color Signal,2012	Generate the indiscriminately prime numbers then storing random keys in matrix. Dividing the image into a collection of blocks.	This planned secret writing algorithmic program will make sure the lossless of transmissions of pictures.	Time overwhelming and additional sophisticated for swapping.
Image secret writing and cryptography by victimization Partition and Scanning Pattern,2012	Secret writing of the particular scan language are partitioned off into four sub-partitioned and every sub-partition are to be scanned severally, wherever a picture is partitioned off within the order once the four sub-partitions are scanned by the partition pattern.	It provides a lossless secret writing of pictures and uses solely number arithmetic and it's simple to implement in hardware.	Complex, Time taking and conjointly possibilities of mistakes are high.
An Improvement over a picture secret writing methodology supported Total Shuffling, 2013.	Chaos and permutation diffusion structure and this paper conjointly conferred an improvement over Eslami's theme.	Quicker than those of while not loss of security. Therefore, the planned methodology is additional possible within the sensible communications.	Lengthy, sophisticated, Time overwhelming and possibilities of mistakes is high.
Modified Algorithms of secret writing and cryptography of pictures victimization Chaotic Mapping2013.	During this paper 2 chaotic based mostly approaches are used they're chaotic baker and chaotic zoologist map.	High sensitivity to secret key has entropy near ideal worth.	Attributable to a lot of mathematical machine, it takes long term to encode the image.
Encryption algorithmic program by victimization Block based mostly trinomial Transformation algorithmic program (Hyper Image secret writing Algorithm) 2013.	First off selected the image are in binary worth blocks then it'll be set up into a permuted image by the victimization the method of permutation and by the victimization of HIEA algorithmic program.	Terribly easy, direct mapping algorithmic program victimization feistal structure. Sensible strength of the secret writing algorithmic program.	Final output, though' obtained properly, isn't clear and comparisons are high therefore time overwhelming.
Image secret writing and cryptography victimization Gradient Technique, 2013.	A technique by victimization a picture secret writing technology that relies on 2 levels particularly intensity variation and component color worth swapping.	Easy arithmetic for manipulations, higher security instead of alternative SKC ways and output image are clear.	Superior and subordinates both the parties are dependent on each other for leaking the whole information.
Dissociable Reversible information concealing in Encrypted Image with Improved Performance, 2013.	Encrypted grayscale image as a reversibly hide the info. Within the 1st part by victimization of secret writing key the owner encode the as a permuting the pixels then the information hider by the bar graph hides the some data within the encrypted image.	Provides the next information capability than the comparisons of the present reversible information concealing technique is in encrypted image and therefore the PSNR is more than the present reversible information concealing technique.	Time taking and risky, no changes in shuffled bar graph, quality of secret writing is low.
Image Steganography in DWT Doman victimization Double-stegging with RSA secret writing, 2013.	Supported the mixture of the 2 options of Cryptography and Steganography.	Double stegging has hyperbolic the info security compared to the opposite modes, and it provides best PSNR values.	Attributable to a lot of decomposition of the many levels, it takes long term to encode the image, prolonged and complex.

A biological science Image secret writing technique supported the RGB constituent shuffling, 2013. .	Image secret writing by shuffling the RGB constituent values.	Effective in terms of the security analysis, increase of security of the image against all potential attacks.	R, G and B Pixels shuffling takes further times then different ways, heap of confusion in methodology, Permutation methodology is simply too advanced, Time taking and conjointly possibilities of mistakes live high.

Table 1: Performance Comparison of Image Encryption Scheme

V. CONCLUSION

After studying the papers, we conclude that some problem in the previous image encryption and decryption algorithms are exists. First of all the majority of encryption algorithms are based on Scrambling algorithms in which pixel exchanging happened. This scheme encrypts the image but cannot change the histogram of an image. So, their Security performances may not good. Some of the techniques are value transformation based algorithm. It changes the pixel value making the image meaningless, but after transformation still the relation between pixels is exists. Also, there is no encryption algorithm exists that can give attention to both the pixel exchanging and gray level exchanging concept. In addition to these there are some other problem exists such as total keys size and computation

Used in previous algorithm is very large. So time complexity is high. On the basis of study of all the above mentioned research papers, the following suggestions can be drawn: To protect multimedia contents, pixel permutation based algorithm should be implemented or used. More complex & compressed algorithm should be used to provide high speed and security to the System. Modified version of various algorithms is used to increase the security level.

REFERENCES

[1] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry, "Efficiency and Security of Some Image Encryption Algorithms", Proceedings of the World Congress on Engineering, London, U.K,.Vol I 2008 .

[2] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, 2006.

[3] Mohammad Ali Bani Younes and Aman Jantan, "an image encryption Approacsh using a combination of permutation technique followed by Encryption", International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[4] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, "Digital image encryption algorithm based On chaos and improved DESǁ", IEEE International Conference on Systems, Man and Cybernetics, 2009.

[5] Ismail Amr Ismail, Mohammed Amin, Hossam Diab "A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.

[6] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation", IEEE International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011.

[7] Yicong Zhou, Sos Agaian, "Image Encryption Using the Image Steganography Concept and PLIP Model", International Conference on System Science and Engineering, Macau, China - June 2011.

[8] Yue Sun, Guangyi Wang, "An Image Encryption Scheme Based on Modified Logistic Map", Fourth International Workshop on Chaos-Fractals Theories and Applications, 2011.

[9] Payal Sharma, Manju Godara, Ramanpreet Singh, "Digital Image Encryption Techniques: A Review", International Journal of Computing & Business Research, 2012.

[10] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012.

[11] Sukalyan Som, Atanu Kotal, "Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps", National Conference on Computing and Communication Systems (NCCCS), 2012.

[12] Gamil R. S. Qaid, and Sanjay N. Talbar, "Encryption and Decryption of Digital Image Using Color Signal", International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012, pp. 588-592.

[13] Monisha Sharma, Chandrashekhar Kamargaonkar, and Amit Gupta, "A Novel Approach of Image Encryption and Decryption by Using Partition and Scanning Pattern", International Journa of Engineering Research & Technology (IJERT), Vol. 1, Issue 7,September 2012, pp. 1-6.

[14] Yong Zhang- Encryption Speed Improvement on "AnImprovement over an Image Encryption Method Based on Total Shuffling", 2013.International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS).

[15] Nadiya P v, B Mohammed lmran et al –" Image Steganography in DWT Domain using Double-stegging with RSA Encryption", 2013 International Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPR].

[16] Rintu Jose-"A Separable Reversible Data Hiding in Encrypted Image with Improved Performance, proposes a novel scheme to Reversibly hide data into encrypted greyscales image in a Separable manner", International Conference on Microelectronics,

Communication and Renewable Energy (ICMiCR-2013).

[17] [Quist-Aphetsi Kester, "A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, January 2013.

