ISSN 2229-5518

K-mean clustering based Video Encryption Technique

Yogita Negi [1], Ravindra Purwar[2]

Abstract— There are various encryption techniques purposed for encrypting videos and used for obtaining highly encrypted videos. This paper consists of brief description about existing methods for video techniques, which focuses on the full or selective encryption techniques.In this paper, a k-mean clustering video encryption has been purposed which uses colour-based segmentation for generation of key images. Each key image is xor-ed with the frame to produce an encrypted frame, finally encrypted frame will be clubbed together to form encrypted video.

Index Terms—Deformation & formation Algorithm, I-frames, chaos, VEA.

1 INTRODUCTION

Due to rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important.

The main goal of cryptography is keeping data secure from unauthorized attackers. Therefore, data is encrypted through process of Encryption. The reverse of data encryption is data decryption

With digital video transmission, encryption technologies are needed that can protect digital video from attacks during transmission. Due to the huge size of digital videos, they are usually transmitted in compressed formats such as MPEG, or H.264/AVC (standard used for video compression) [8].

2 NEED OF VIDEO ENCRYPTION

Encryption of images and videos are important due to following reasons:
1. For preventing unwanted viewing of transmitted video, for example from law enforcement video surveillance being relayed back to a central viewing centre.
2. To protect the private multimedia messages that is exchanged over the wireless or wired networks.
3. Video Encryption is helpful in securing videos used in services like video on demand (VOD), Video conferencing-learning.
4. For protecting medical videos which may contain private information of a patient from unauthorized access by malicious users.
In first section of this paper, the basic concept of video encryption is discussed, then second section of this paper, covers various approaches of video encryption. Again, third section of this paper, deals with constructing and implementing new algorithm based on K-mean clustering based video encryption. Last section of this paper, covers the security issues related to the image encryption that is depicted using histogram of original & encrypted image.

3 BASIC CONCEPT OF VIDEO ENCRYPTION

The encryption and decryption of a plain text or a video stream can be done in two ways:

3.1 SECRET KEY ENCRYPTION:

A single secret key can be used to encrypt and decrypt the video streams. Only the sender and the receiver have this key. Basically, the security level of the symmetric keys encryption method is totally depends on how well the users keep the keys protected. If the key is known by an intruder, then all data encrypted with that key can be decrypted. Most common algorithms in these categories are Data Encryption Standard (DES), Triple DES, and Advance Encryption.

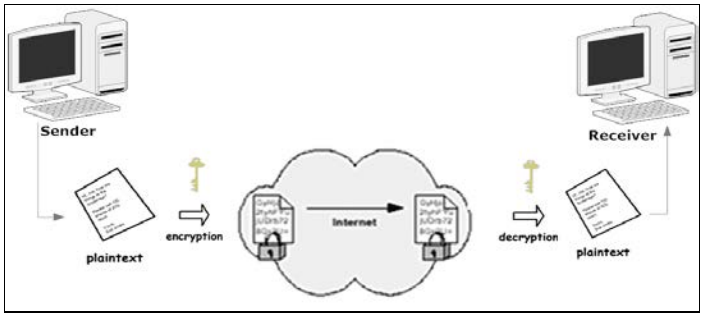

Fig.1 Symmetric key Algorithms [1]

3.2 PUBLIC KEY ENCRYPTION:

There are two keys, one for encryption and the other for decryption. The public key, which is known for all senders, is used for encryption. While the private key, which is owned only by the receivers, is used for decryption. [2]
It is based on a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and solves the problem of secret key distribution by using two keys instead of a single key .

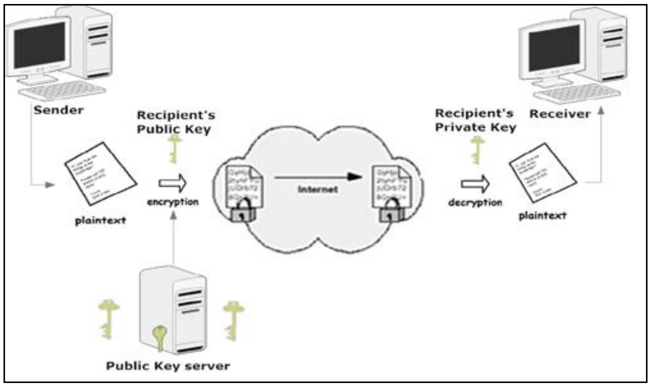

Fig.2 Asymmetric key Algorithms [1]

4 VARIOUS APPROACHES USED FOR ENCRYPTION:

4.1 FULL-ENCRYPTION:

A video encryption algorithm that performs encryption on the entire video bit stream belongs to this class of algorithms.
It is suitable for real time video as requires heavy computation and has slow speed. This class of algorithms includes the naïve approach. The naïve approach is a type of full encryption approach in which a conventional cryptosystem is used in the encryption step. All other full-encryption approaches that are not using a conventional, general-purpose cryptosystem are grouped into non-conventional full-encryption approaches.
These non-conventional approaches are designed mostly to accommodate low computational complexity and fast performance.
Chaos-based video encryption algorithms, as well as the approaches proposed in this dissertation are examples of such algorithms. [8]

4.1.1 NAÏVE APPROACH:

It is a type of full encryption approach in which a conventional cryptosystem is used in the encryption step. The most straight-forward method to encrypt every byte in the whole Moving Picture Experts Group (MPEG) stream using standard encryption schemes such as DES or AES.
However, this algorithm not applicable for heavy video, because it is very slow especially when we use triple DES. Because of the encryption operation the delay increases therefore it is not suitable for real time video encryption. [1]

4.1.2 Chaos Based Encryption Approach:

This is one of the popular algorithms in the field of neural network to perform encryption & decryption as it is a low cost algorithm & is suitable for large amount of data.
The chaos-based image cryptosystem mainly consists of two stages [21].
The plain image is given at its input. There are two stages in the chaos- based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognisable. The pixel permutation is carried out by a chaotic system. The chaotic behaviour is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image an important tool to protect image from attackers.

4.1.3 Pure Permutation Algorithm:

The idea of pure permutation algorithm is simply scrambles bytes within a frame of MPEG stream by permutation. It is extremely useful in situation where the hardware decodes the video, but decryption must be done in software. [2]

4.1.4 Zig-Zag Permutation Algorithm:

In this method, instead of mapping the 8x8 block to 1x64 vector in “Zig-zag” order, it maps the individual 8x8 block to a 1x64 vector by using a random permutation list (secret key).
There are many ways to produce a permutation list which has uniform distribution over all possible permutations. This algorithm consists of three steps:
i) Generate a permutation list with cardinality 64.
ii) Complete splitting procedure after 8x8 blocks is quantized.
iii) Apply the random permutation list to the split block, and pass the result to the entropy coding procedure. [2]

4.2 Selective Encryption:

Also known as partial encryption & is a subcategory of variable encryption. The algorithms in this class selectively encrypt the bytes within video frames. As these algorithms are not encrypting each and every byte of video data, it reduces computational complexity.
This class of video encryption algorithms consists of all approaches that perform encryption only on certain, carefully selected bits from the video bit-stream (compressed or uncompressed), while leaving the rest of the bits unencrypted. Even more generally, one can define variable encryption to be an approach where different encryption security levels are applied to different bits from the input.[8]

4.2.1 Deformation & formation Algorithms:

In this form, encryption using key image is used perform full encryption process. In this new scheme for video encryption which based on encryption of I-frame (video frame).

4.2.1.2 Deformation Algorithm:

- In this method, a video Vi is divided into I1, I2...In (where n=1, 2…..n) video frames such as frames are collected then take frame one by one.
- Then, select two key Images namely K1, K2 as key frames for encryption and decryption process, so this key images can be send through secure channel.
- Each frame has dimension of "w* h".
- Let αi denotes any sorting permutation like quick sort, heap sort of Ii & α(Ii) is image with sorted pixels from 'Ii'.
- Video stream is collection of still images & these images are refereed as I-frames.
- Here ,first frame is not encrypted & is transmitted through secure channel whereas
- Second frame is xored with second key image, K2.Again the output is xored with sorted value of first frame.
- The process is repeated for all frames till encrypted video sequences E1, E2….En are generated.

4.2.1.3 Formation Algorithm:

For decrypting the obtained sequence of encrypted video following steps are followed [5]:

- Receive all frames of videos along with key images: K1, K2.
- Each frame E1 is xored with first key image K1 & again the output is xored with its previous frame i.e first frame initially.
- Then the output is xored with key image K2 to obtain first I-frame of video.
- These steps are repeated for all the encrypted frames E1, E2...................En (where n = 1,2…..n.)
- Finally construct the final video (consisting of I1,I2...........In frames) by collecting all the frames.

4.2.1. Video Encryption algorithm (VEA):

In this concept, this new encryption will divide the input videos streams into odd chunks(a1, a3, a5, …. , a2n-1) and even chunks(a2,a4,….a2n) & then encryption key would be applied to the even list E(a2, a4,a6, … , a2n), where E denotes an encryption function.

5. PURPOSED K-MEAN CLUSTERING BASED VIDEO ENCRYPTION:

In this paper, a new scheme for video encryption has been purposed based on encryption of I-frame (video frame).In this method, we convert entire video into different frames and then take each frame one by one to apply encryption in it and again, we select 3 Images as key images (frame) that are based on color k-means clustering used in color segmentation for encryption and decryption process, where key image will be send through secure channel. An encryption algorithm is applied to all the frames & then it will combine all frames to make video which is in encrypted form.

- Consider a video sequence V that consists of consisting of n frames denoted by I1, I2…In.
- Now each frame has a dimension of w ×h and up to 2n different pixel values (colors).
- Finally, again a function generator F(i) for Ii .For a given frame I, there are three secret key images generated for frame Ii.
- By utilizing concept of color segmentation based on k-means clustering, 3 key images are produced.
- Function generator known to any two distant parties can compute solely by knowing a F(Ii), which is the case when the parties utilize the same computational method.
- The entire procedure of encryption is shown through an encryption algorithm.

K-MEAN CLUSTERING BASED VIDEO ENCRYPTION ALGORITHM:

- In this method, a video Vi is divided into I1, I2...In (where n=1, 2…..n), video frames such as frames are collected then take frame one by one.
- Then, select three key Images namely K1, K2, K3 as key frames for encryption and decryption process, so this key images can be send through secure channel.
- Each frame has dimension of "w* h".
- Let Fi denotes any Key generation function based on k-mean clustering color segmentation of frames of Ii.
- Video stream is collection of still images & these images are refereed as I-frames.
- In this algorithm, first frame is not encrypted & is transmitted through secure channel whereas Second frame is xored with third key image K3.
- Then, first output, Cn is xored with I(n-1.)
- Again, second output Dn, is produced by xoring frame with key frame K2.
- Again second and third output is xored to produce, Fn.
- Further Fn, is xored with key frame K1 to produced encrypted frame, E2.
- The process is repeated for all frames till encrypted video sequences E1, E2….En are generated.

5.1 ALGORITHM (ENCRYPTION):

1. Given a video sequence V =I1, I2, I3………In.

```
2.  From the given video V, compute all frames V =I1, I2, I3………In.
3.  Compute key frames K1, K2, K3 using function Fi=function generator based on k-mean color segmentation.
4.  For all the frames from Ii ,i=2,……...n, perform following:
5.  (a)K1, K2, K3 =Fi( frame I1) where K1 ,K2,K3 are key images with different color intensity. Send them through secure channel.
6.   Cn=(In xor K3) where n = 2,3,4,….n
     Dn=(Cn xor In-1)
     Gn=(Dn xor K2)
     Fn=(Dn xor Gn)
     En=(Fn xor K1)
7. Repeat step 5. for the remaining all frames.
8. Reconstruct the video sequence using encrypted
   Frames.
9. A regular non secure channel R can be used for
   the  transmitting this video.
10. A secure channel is required to transmit key
   frame Ii,Fi(key frame generator),Key frames K1,K2,K3.
```

For decrypting the obtained sequence of encrypted video following steps are followed :
Receive all frames of videos along with key images K1, K2, K3:

- Each frame E2 is xored with key image K3 & again the output D2 is xored with A to obtain C2 frame.
- Then, the output C2 is xored with key image K1 to obtain original I-frame of video.
- These steps are repeated for all the encrypted frames E1, E2…….En (where n = 1,2……..…..n.)
- Finally construct the final video (consisting of I1, I2……...In frames) by collecting all the frames.

5.2 ALGORITHM (DECRYPTION):

```
1.  Obtain a Encrypted video frames E1,
     E2, E3……………………………En.
2.  First frame Ii, Keys K1, K2, and K3.
3.  Compute all frame of video.
4.  Fn = ( En xor K1) where n = 2,3,4,….n
    Gn = ( Fn xor Dn)
    Dn =( Gn xor K2)
    Cn=(Dn xor In-1)
    In= (Cn xor K3)
5.  Repeat step 3. for the remaining all frames.
```

6. EXPERIMENTAL RESULTS/SIMULATION

1. Algorithm implemented on rhino.avi

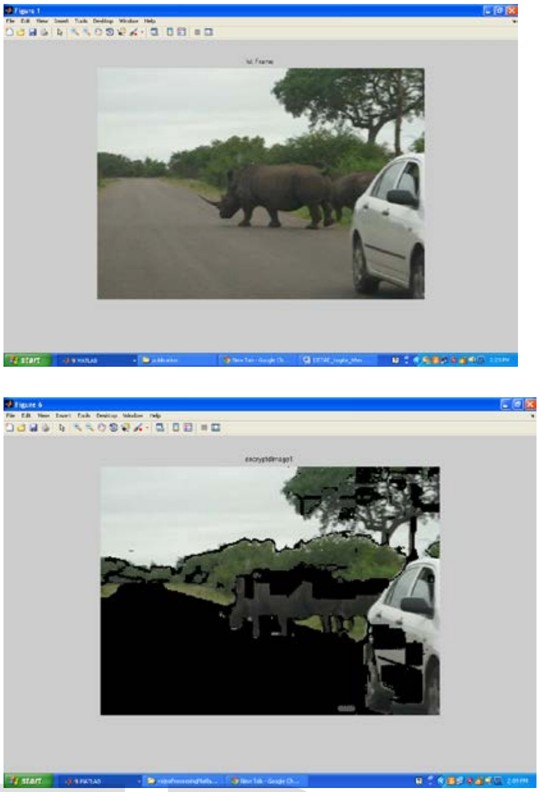

Figure.3 Encryption result by proposed algorithm: (a) original image; (b) encrypted image

2. Algorithm implemented on gymnastic.avi

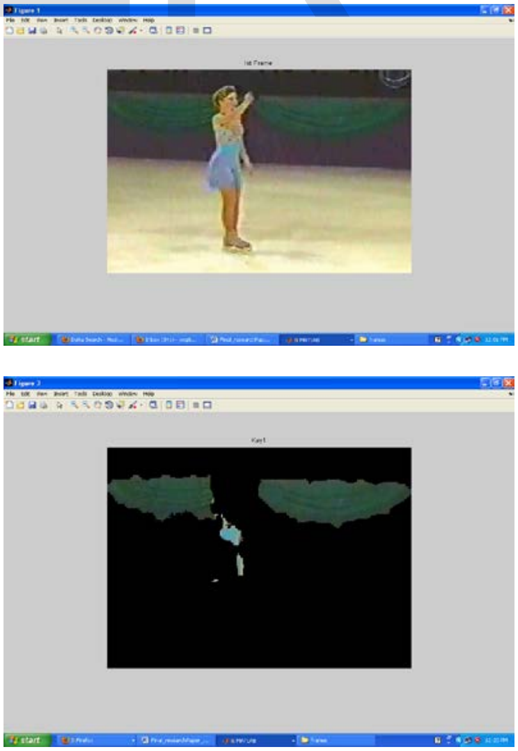

Figure4 Encryption result by proposed algorithm: (a) orig-

inal image; (b) encrypted image

7. Security Analysis

To test the robustness of the purposed scheme, security analysis was performed. Following factors are responsible to test security analysis:

7.1. IMAGE HISTOGRAM:

It illustrates how pixels in an image are distributed by graphing the number of pixels at each colour intensity level. It is observed that the histogram of the final encrypted image is fairly uniform and is significantly different from that of the original image.

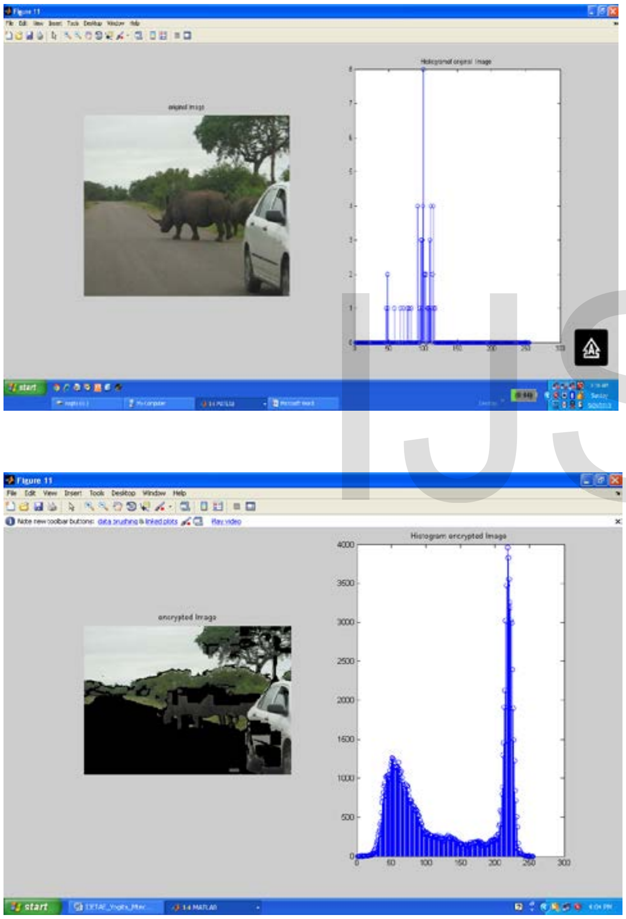

Figure. 5 (a) Histogram of original image; (b) Histogram of encrypted

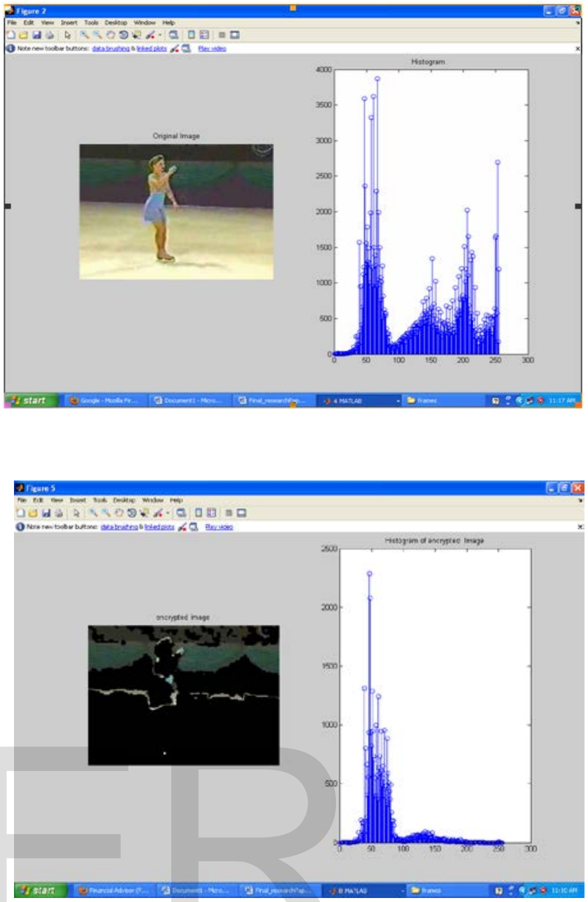

Figure. 6 (a) Histogram of original image; (b) Histogram of encrypted image

8. Conclusion:

This paper focuses on the various methods for Video Encryption. From the above analysis, the following conclusions have been drawn:

- Amongst the two approaches: selective encryption takes less time as compared to full encryption.
- Zigzag method & chaos based method are hot research topics for encryption of video but takes more time.
- Therefore, a new encryption algorithm based on K-means clustering of I-frames is evolved, that helped to encrypt the video frames.
- Again we analysed security aspects of the proposed method, and show that the method is efficient and secure from a cryptographic point of view.

References

[1] M. Abomhara,, Omar Zakaria, Othman O. Khalifa “An Overview of Video Encryption Techniques”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.

[2] Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey", International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.

[3] Amit Pande, Prasant Mohapatra, Joseph Zambreno," Using Chaotic Maps for Encrypting Image and Video Content", 2011 IEEE International Symposium on Multimedia.

[4] Sufyan T. Faraj Al-Janabi, Khalida Shaaban Rijab, Ali Makki Sagheer," Video Encryption Based on Special Huffman Coding and Rabbit Stream Cipher", 2011 Developments in E- systems Engineering.

[5] Mayank Arya Chandra, Dr. Ravindra Purwar, Dr. Navin Rajpal,"A Novel Approach of Digital Video Encrytion", International Journal of Computer Applications (0975 – 8887) Volume 49– No.4, July 2012.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based for Image Encryption", World Academy of Science, Engineering and Technology 3 2007.

[7] Fadi Almasalha,Ashfaq Khokkar,Rogelio Hasimoto beltran,"Scalable Encryption of variable Length Coded video Bit Streams",35th Annual IEEE conference on Local Com.

[8] Daniel Soek,Hari Kalva,Syyros S. Magliveras,"New Approaches to encryption and steganography for digital videos",Multimedia Systems,D01 10.1007/ s00530-007-0083- z,@Springer-Verlag 2007.

[9] Knuth, D.E.: The art of computer programming, 2nd edn., vol. 3: Sorting and Searching, pp. 113–122. Addison–Wesley, Reading, A (1998).

[10] S.Chen, G., Zheng, X.,"Multimedia security handbook. Internet and Communications Series, vol. 4, chap. Chaos-Based Encryption for Digital Images and Videos", pp. 133–167. CRC Press, West Palm Beach (2004).

[11] X.,Eskicioglu,A.M.:, "Selective encryption of multimedia content in distribution networks: Challenges and new directions.", In: Proceedings of the Second IASTED International Conference on Com munications, Internet and Information Technology (CIIT 2003), pp. 527–533. Scottsdale, AZ, USA, IASTED, 17–19 November 2003.

[12] ISCAS 2004. 2004. 3. Guosheng Gu, g.H." The application of chaos and DWT in image scrambling. in Proceeding of the Fifith Interational Conference on Machine Learning and Cybernetics", 2006.

[13] Dalian S. Agaian, J.A., K. Egiazarian, P. Kuosmanen, "Decompositional methods for stack filtering using Fibonacci pcodes. Signal Processing," 1995.

[14] David. Gevorkian, K.O.E., Sos S. Agaian, "Parallel Algorithms and VLSI Architectures for Stack Filtering Using Fibonacci p-Codes. IEEE Transactions on Signal Processing", 1995,286-295.

[15] Tzouveli Paasikivi, Ntalianis Klimis, Kollias Stefanos "Security of Human Video Objects by Incorporating a Chaos-Based Feedback Cryptographic Scheme".

[16] Daniel Socek,Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk, Borko Furht "New approaches to encryption and steganography for digital videos" ,Springer-Verlag 2007.

[17] MPEG,1988,"The MPEG Home Page. Retrieved Jan 13, 2009, from http://www.chiariglione.org/mpeg/"

[18] Chang Wen Chen, Senior Member, IEEE, Jiebo Luo, Member, IEEE, and Kevin J. Parker, Fellow, IEEE, "Image Segmentation via Adaptive –Mean Clustering and Knowledge-Based Morphological Operations with Biomedical Applications", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 7, NO. 12, DECEMBER 1998

[19] Yining Deng, B. S. Manjunath and Hyundoo Shin*,"Color Image Segmentation",Department of Electrical and Computer Engineering University of California, Santa Barbara, CA 93106-9560 *Samsung Electronics In{deng, manj, hdshin}@iplab.ece.ucsb.edu.

[20] Mushir Ahmed,"A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", Musheer Ahmad et al /International Journal on Computer Science and Engineering, Vol.2(1), 2009, 46-50.

[21] K.Sakthidasan @ Sankaran and B.V.Santhosh Krishna," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images",International Journal of Information and Education Technology, Vol.1,No. 2,June 2011.