ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Providing Protection on Cloud Video Surveillance Using Blowfish Algorithm

Swati Suryawanshi [1], Vaishali Kolhe [2]

M.E. Student, Department of Computer Engineering, D. Y. Patil College of Engineering, Akurdi, Savitribai Phule Pune University, India[1]

Associate Professor, Department of Computer Engineering, D. Y. Patil College of Engineering, Akurdi, Savitribai Phule Pune University, India[2]

ABSTRACT: In the today's world, the multimedia data like images, videos, texts are stored on cloud. In cloud, security is a great challenge as data is transmitted through internet and saved on third party server. Surveillance systems usually use cameras to capture all the activities in the environment. Data generated by the video surveillance system is transmitted to cloud server through internet. For providing security to video surveillance system, video is encrypted while uploading and decrypted after downloading by using blowfish algorithm. Blowfish algorithm is designed for encryption and decryption of images using a secret key block cipher which is used to increase the security and improve the performance. This algorithm is used the variable key size up to 448 bits. It used the Feistel network which iterates function 16 times. Performance of data uploading to cloud server improved by compressing the data and security improved by using blowfish algorithm.

KEYWORDS: Cloud Computing, Video Surveillance, Privacy Protection, Cryptography, Encryption, Decryption, Blowfish Algorithm.

I. INTRODUCTION

The cloud computing is growing fast because the cloud based applications are increased. The multimedia data produced in a large amount so it is stored in the cloud. The confidential information in the cloud, where the user loses the control of their information, so the security risk is increased [1]. The user can provide the security to data from unauthorized access by using encryption technique.

Video surveillance systems are widely used to battle the rapidly increasing security threats. In these systems, a large number of cameras are deployed to extend the coverage. These cameras capture all the activities happening in the environment, which should be examined for the situation [2].

The unauthorized users can be accessed the secured data during data transmission via internet. So for providing the protection from unauthorized access, Encryption algorithm was implemented. In Encryption, the data is converted into the unreadable format and which is accessed only by the authorized user having the key. Image security is very important because of web attacks are increases. Images are used in many fields like video calling, military communication, medical system, multimedia system, etc [3]. There are various techniques provided for security purpose at the time of store and transfer images. So the cryptography is used to provide the security to confidential data on to the cloud.

The word cryptography originates from the Greek words; it is used for hiding confidential data. The term cryptography is used to write the secret messages with the image, so the original image is hidden and manages the security well [4]. It is used for sending messages between sender and receiver privately. Encryption is the process which used the algorithm to transfer the data over the internet in unreadable format to prevent from hackers. There are two types of encryption are there the symmetric-key encryption and asymmetric–key encryption [5]. The symmetric-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

key means the same key is used for both encryption and decryption. The asymmetric-key encryption different keys are used for encryption and decryption.

In the existing paper first, the face is detected after that the scrambling algorithm is applied on detected faces and create the video and it sent on to the cloud. After downloading the video from cloud to apply the R-Prime Shuffle algorithm and get the original video back [6]. But it takes a lot of time for all the process done and it only hides the privacy region which is detected by face detection technique which is not properly secured. Because the remaining video is displayed as it is so it can be easy for hackers to assume the original contents. The R-Prime shuffling algorithm is used there so after guessing key it is very easy to unscramble it so it is the drawback of this scrambling algorithm. To provide the strong security the encryption algorithm is used in the proposed system [7].

In the Proposed system the blowfish algorithm is a very fast algorithm and best option for secure the images [8]. Blowfish algorithm is much fast and has not been broken yet; it is composed in an approach to satisfy every one of the perspectives.

Speed: DES algorithm is slower than Blowfish algorithm. The block size in Blowfish algorithm is 64 bits. The length of the key is variable up to 448 bits.

Compactness: It is working in less memory space, this space may be under 5K.

Simplicity: It performs a simple operation like addition, exclusive-or, and table queries.

Flexibility of key size**:** The key in Blowfish algorithm doesn't change frequently [9].

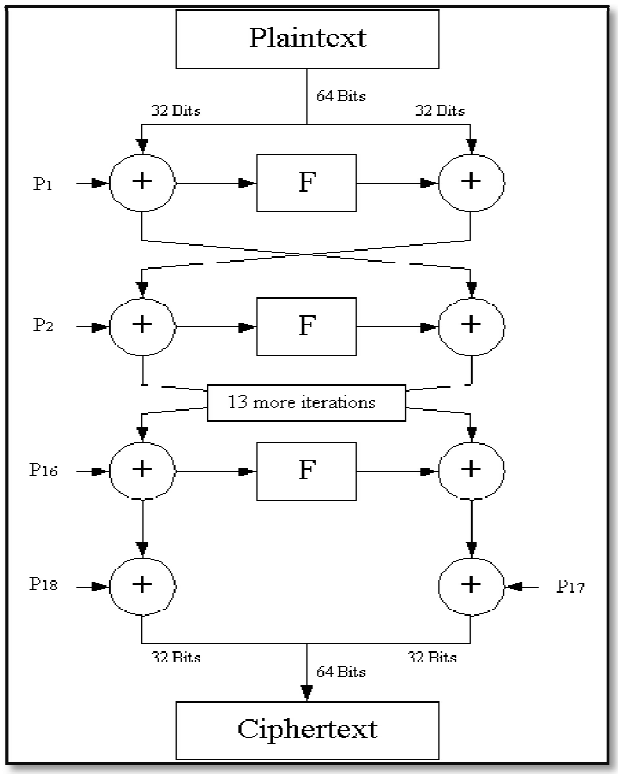

Fig.1 The Feistel Structure of Blowfish.

The blowfish algorithm encrypts 64-bits of the data block at once. It is used after Feistel network. It consists of P-arrays and S-boxes. Eighteen 32-bits boxes are given by P-array and four 32-bits array given by S-boxes, both of these have 256 entries each. All tasks are XORs and increases on 32-bit words. There is also an addition operation that is four indexed array data queries for each round.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Section I defines introduction about proposed system, section II includes Literature Review and section III includes System overview, section IV describes Result analysis and section V includes conclusion.

II. RELATED WORK

1. Image encryption and decryption using blowfish algorithm in matlab. This paper [3] presents the encryption algorithm is used to convert the data into the unreadable format and which is accessed only by the authorized user having the key. Image security is very important because of web attacks are increases. Images are used in many fields like video calling, military communication, medical system, multimedia system, etc. There are various techniques provided for security purpose at the time of store and transfer images. So the cryptography is used to provide the security to confidential data on to the cloud.
2. Cryptography in Image Using Blowfish Algorithm. The authors in [4] presents securing the image is executed with a Blowfish algorithm from the perspective of cryptology. Blowfish is used for the applications, where the key doesn't change often and has a larger space to store the data. Encryption and decryption is performed to obtain the original hiding information from the image. Blowfish is the strongest algorithm, it cannot compromise the security.
3. Secure non real time image encryption algorithm development using cryptography Steganography. This paper [10] presents the today's world, data transmission of various multimedia like sensitive images, videos, texts are very important and security is most important in the medical, commercial and military fields. Now a day's, many techniques are available for secure transmission of data through internet like cryptography. In this paper Image encryption is done using Blowfish Algorithm as it is faster and has good performance.
4. Literature Survey on Different Techniques of Image Encryption. This paper [9] represents Encryption is used to transmit data securely in open networks. The term cryptography is used to write the secret messages with the image, so the original image is hidden and manages the security well . It is used for sending messages between sender and receiver privately. Encryption is the process which used the algorithm to transfer the data over the internet in unreadable format to prevent from hackers. There are two types of encryption are there the symmetric-key encryption and asymmetric-key encryption. The symmetric-key means the same key is used for both encryption and decryption. The asymmetric-key encryption different keys are used for encryption and decryption.
5. Fully Reversible Privacy Region Protection for Cloud Video Surveillance. This paper [12] proposed a privacy region protection scheme for cloud video surveillance which allows full recovery of the original H.264/AVC compressed videos recorded at the camera. The quantized DCT coefficients in the privacy region are scrambled based on their drift influence on the non-privacy region. Thus the intra-frame error drift in the privacy region is maintained to facilitate the protection of the visual security of the privacy region, but vanish in the non-privacy region. The main advantages of the proposed scheme are its full reversibility and its low computational cost.
6. A Review on DES, AES and Blowfish for Image Encryption Decryption. In this paper [13] the authors discussed and surveyed DES, AES and Blowfish for Image Encryption and Decryption. In today's world it is a crucial concern that while transferring image from one network to another over the internet, the proper encryption and decryption should be applied so that unauthorized access can be prevented. The authors also surveyed related re-search and did some problem identification and provided suggestions that can be useful for image encryption. This is to enhance the performance and encryption and decryption times of the image.

III. SYSTEM OVERVIEW

The main objective behind the outline of this proposed system is to get the best security/performance exchange off over existing system by utilizing blowfish algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

A. *System Architecture:*

Figure 2 shows system architecture. First, user and admin login to the system, after authentication user can start the web cam.

1) Detect Image: Image detection conditions are as follows:
   a) If webcam set to 0 then internal camera of a computer is detected.
   b) If webcam set to 1 then the external camera is detected.

2) Capture Frames: Whenever web camera is started then web camera captures the images and those images are stored in file system. Our system detects camera b
3) ased on an index and those index based on web camera. By default 0 indexes are assigned to default camera in the system.

4) Encryption and Decryption: The original image which is captured by a web cam in the form of frames is encrypted by using blowfish algorithm. And at the time of decryption by using the same algorithm we can decrypt frames and get original frames back.

5) Database: Mysql database is used for store the metadata of video. Admin always check in the database user send any request for video or not.

6) Upload and Download video on the cloud: Drop box is an open source cloud provider and it provides maximum 2GB space in the cloud. The need is only create an application in a cloud for integrating our application with the cloud. Example: - For creating keys we need to create our own app in Drop box then Drop box will give API secret keys. While uploading video to drop box, video is compressed and while downloading from drop box, video is uncompressed.

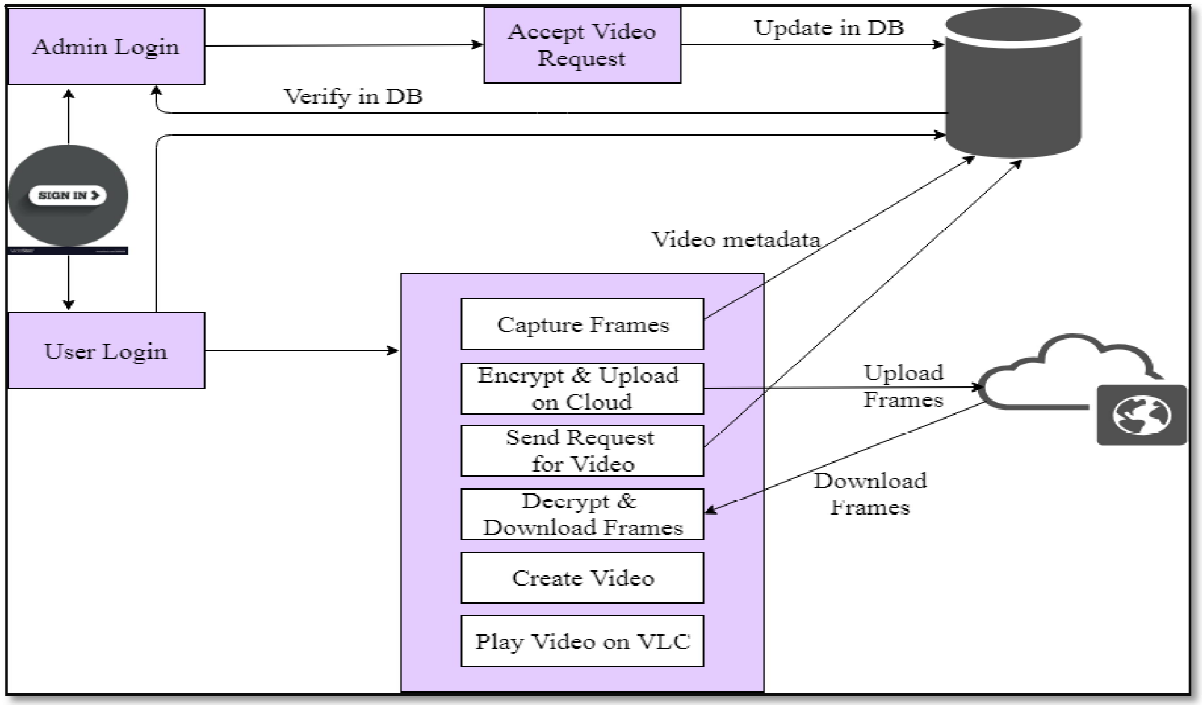

Fig. 2 System Architecture.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

B. *Blowfish Algorithm*

Input: byte array (image converted into array)
output: cipher text

1. *Key Expansion*

Blowfish used large number of sub keys.
The p-array consists of 18, 32-bit sub-keys:
P1, P2,., P18
Four 32-bit S-Boxes consist of 256 entries each:
S1, 0, S1, 1,. S1, 255
S2, 0, S2, 1,.. S2, 255
S3, 0, S3, 1,.. S3, 255
S4, 0, S4, 1 .....S4, 255

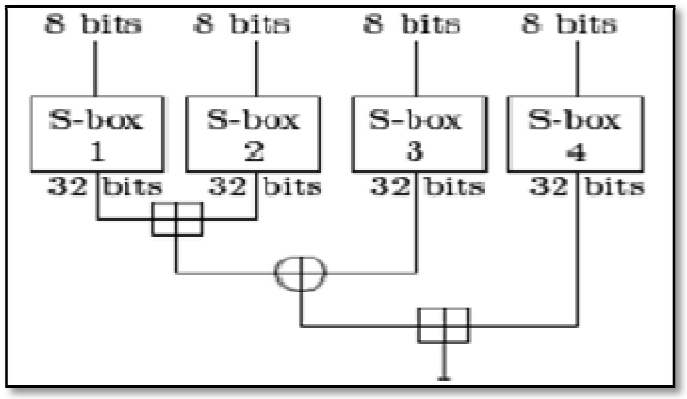

Fig. 3 The Feistel Function of Blowfish.

- *Generating the Sub-keys:*

The sub-keys are calculated and generated using the Blowfish algorithm:

1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3):

   P1 = 0x243f6a88,
   P2 = 0x85a308d3,
   P3 = 0x13198a2e,
   P4 = 0x03707344, etc.

2) XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits.
3) Encrypt the all-zero string with the Blowfish algorithm, using the sub keys described in steps (1) and (2).
4) Replace P1 and P2 with the output of step (3).
5) Encrypt the output of step (3) using the Blowfish algorithm with the modified sub keys.
6) Replace P3 and P4 with the output of step (5).
7) Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

2. *Blowfish Encryption:*

In Encryption, data is divided into two blocks and each blocks is 32 bit.
Divide x into two 32-bit halves: xL, xR
For i = 1 to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR.

3. *Blowfish Decryption:*

Decryption is exactly the same as encryption, except that P1, P2, , P18 are used in the reverse order. This is not so obvious because XOR is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm.

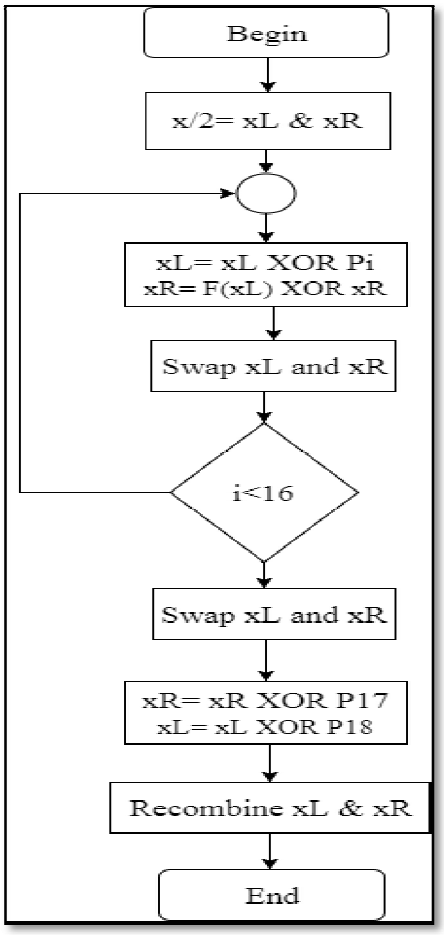

Fig. 4 Data Flow Diagram of Data Encryption [5].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

IV. RESULT

The proposed algorithm has been developed in Java language and various images are used to test the performance of the proposed system. The table I is given below for the comparison between R-Shuffling and Blowfish Algorithm.

Table 1: Comparison Between R-Prime Shuffle and Blowfish Algorithm for Execution

Image name	Size	R-Shuffling Scrambling Time in sec	R-Shuffling Descrambling Time in sec	Blowfish Encryption Time in sec	Blowfish Decryption Time in sec
Book.jpg	11.50 KB	1.5555	0.813	0.19449	0.04250
Education.jpg	10.25 KB	1.2578	0.657	0.12556	0.03589
Signature.jpg	6.00 KB	0.7862	0.5987	0.06685	0.02583
Flower.jpg	9.00 KB	1.0689	0.879	0.10678	0.03357

Blowfish algorithm runs faster as compared to the referred papers algorithms. In the given table the execution time for encryption and decryption for the same images are given in seconds. Every file takes different time for encryption and decryption, so execution time is also different. To prove the efficiency of the proposed algorithm the performance factor such as time is observed.

Fig 5 shows the final graph of execution time for comparison of the proposed algorithm and existing algorithm, where the x-axis represents algorithms and the y-axis represents Execution time (in Second) where a time required for encryption and decryption of proposed algorithm is less than the existing algorithm, So the performance is increased by time for the proposed system.

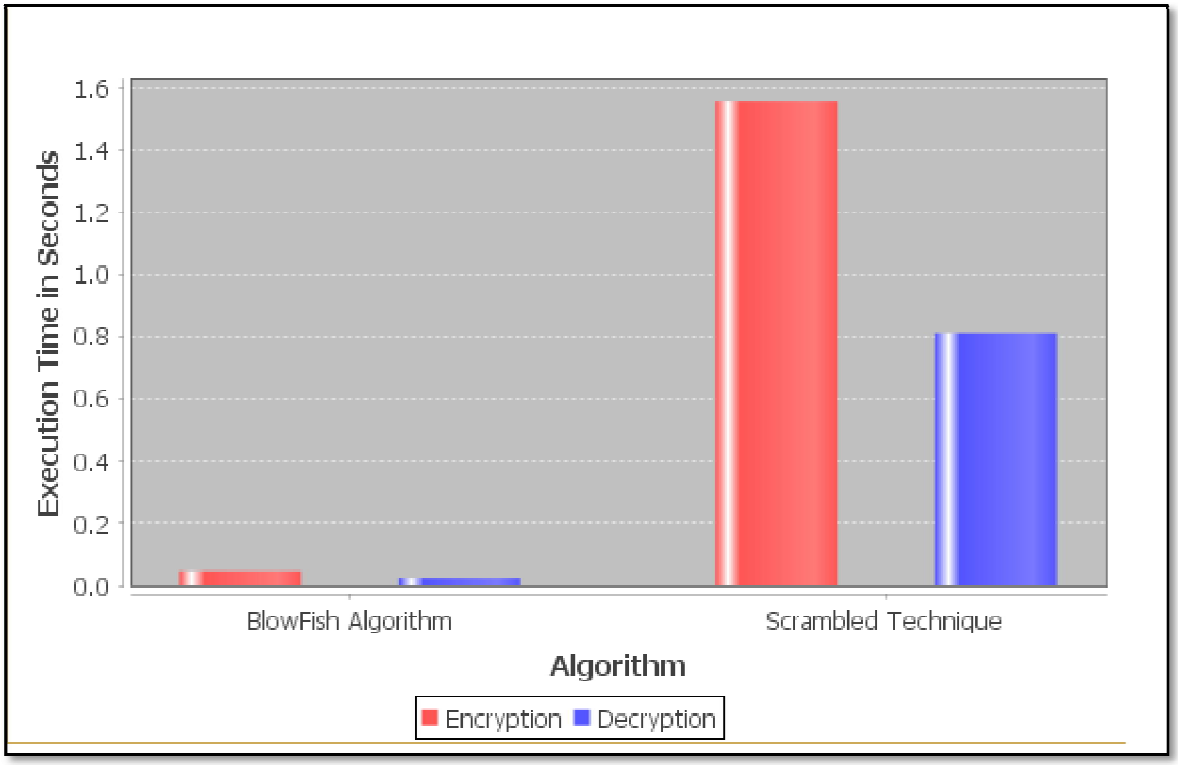

Fig.5. Comparison of speed performance of proposed and existing approach.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

V. CONCLUSION

The privacy protection of the images is very important because of increasing the attacks on the videos surveillance system and cloud. In referred papers, they used the scrambling technique to provide the security to the videos which are stored on to the cloud and after downloading the video unscrambled it and get the original video back but it takes more time. The scrambling algorithm only protects privacy region so it is very easy for the hacker to get original data. In the proposed system, this problem is solved by using the Blowfish algorithm. It is the very strong algorithm for image encryption; it handles the security and privacy of cloud storage to protect the data stored in the cloud. Blowfish cannot be hacked easily until to find the exact combinations of the lock.

REFERENCES

1. Surveillance Society: New High-Tech Cameras Are Watching You Popular Mechanics.[Online].Available: http://www. popular mechanics.com/technology/military/4236865.
2. Mukesh Saini, Xiangyu Wang, Pradeep K. Atrey, and Mohan Kankanhalli. “Adaptive Workload Equalization in Multi-Camera Surveillance Systems.” IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 14, NO. 3, JUNE 2012.
3. Pia Singh “Image encryption and decryption using blowfish algorithm in mat lab. International Journal of Scientific Engineering Research, Volume 4, Issue 7, July-2013.
4. S. S. Sudha, S. Divya “Cryptography in Image Using Blowfish Algorithm. International Journal of Science and Research (IJSR), Volume 6, Issue 4.4, 2013.
5. K. Kanagalakshm, M. Mekala “Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key.” International Journal of Computer Applications (0975 8887) Volume 146 No.5, July 2016.
6. Q. A. Kester, “Image Encryption based on the RGB PIXEL Transposition and Shuffling,” I. J. Computer Network and Information Security, 7, in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijcnis.2013.07.05, pp.43-50, Published Online June 2013.
7. H B Kekre, Tanuja Sarode, Pallavi Halarnkar, “Image Scrambling using R-Prime Shuffle,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 8, August 2013.
8. Bruce Schneier “The Blowfish Encryption Algorithm.” http:// www.schneier.com/ blowfish.html, October 2008.
9. Anjaneyulu GSGN, Pawan Kumar Kurmi, Rahul Jain, “Image Encryption And Decryption Using Blowfish Algorithm With Random Number Generator.” Anjaneyulu GSGN* et al. International Journal Of Pharmacy TechnologyIJPT— Jan-ISSN: 0975-766X, 2014.
10. Moresh Mukhedkar, Prajkta Powar, Peter Gaikwad. “Secure non real time image encryption algorithm development using cryptography Steganography.” in IEEE INDICON 2015, 1570203491.
11. Mohammad Ali Bani Younes “Literature Survey on Different Techniques of Image Encryption.” International Journal of Scientific Engineering Research, Volume 7, Issue 1, 93 ISSN 2229-5518, January-2016.
12. Xiaojing Ma, Laurence T. Yang, Yang Xiang, Wenjun Zeng, Deqing Zou, and Hai Jin, “Fully Reversible Privacy Region Protection for Cloud Video Surveillance.” IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 5, NO. 3, JULY-SEPTEMBER 2017.
13. A. Devi , A. Sharma, and A. Rangra, “A Review on DES, AES an Blowfish for Image Encryption Decryption,” Aarti Devi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, Issue. 3, pp. 3034-3036. http://www.ijcsit.com/, 2015.