IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Ameliorate Large Video Enigma for Promulgation

Dinesh S[1]*, Padmavathi H G[2], C.S. Madhu[3*], Divyashree H S[4], Bharath Raj D[5]

[1]Department of Information Science & Engg, Brindavan College of Engineering, Bangalore, India
[2,3,4]Department of Computer Science & Engg, Brindavan College of Engineering, Bangalore, India
[5]Department of Information Science & Engg, Brindavan College of Engineering, Bangalore, India

**Corresponding Author: sdineshgowda@yahoo.co.in*

DOI: https://doi.org/10.26438/ijcse/v7i2.596600 | Available online at: www.ijcseonline.org

Accepted: 18/Feb/2018, Published: 28/Feb/2019

***Abstract*:** The usability of images and videos is increased in a remarkable speed which built the fear of insecurity in the minds of end users. To revamp the security and bandwidth, allocation, while promulgation of data. A new concept has put forward to provide two levels of security by minimizing the size of the video using the compression algorithm and to encrypt it by using the Blow fish algorithm. This proposed Algorithm takes less memory Uses simple operations like XOR and additions, This algorithm improves significant efficiency**.**

Keywords*–Promulgation, Feistal network, Key expansion ,Enigma*

I. INTRODUCTION

Cryptography is the study of techniques for securing the data from the third parties. It is also responsible for novicenormal message to secure message and vice versa. More generally, cryptography is process of forming and inspectingprotocols that avoid unauthorized parties from accessing secret messages

Cryptography is a vital an essential part in protection of information amongst sender and beneficiary. Cryptography gives us analysis, correctness, civility, alongside information uprightness. Presently the cryptography is used in communications by spy's military leaders routinely to secure information, which must be imparted and/or spared over long stretches, to ensure electronic asset exchanges and grouped interchanges.

With the increasing growth of multimedia applications, preservation is an important issue in transmission of images. Encryption is one the way to ensure security. Image encryption techniques convert original image to another image which is hard to understand. Also reliable security in storage and transmission of digital images is needed in many applications, such as online personal photograph album, medical systems, confidential video conferences, military communications etc.In order to fulfil such a task, many video encryption methods have been proposed. Encryption is the process of encoding messages or information in such a way that only restricted parties can able to understand it using the decryption key

The data security expresses much significance in exceptionally field of life. Particularly the Military undertakings and private business are acutely touchy in such manner. To keep the data away from the reach of unauthenticated clients or to make it safe from being corrupted is called data security. Encryption is animperative security component.

The fundamental method of working is to crumble the data into incomprehensible data and afterwards unscrambles it for perusing utilizing a key. Encryption of the content (text) is not quite the same as that of an image. Because of the natural characters of images, for example, mass information limit and high excess, encryption on picture or video objects has its own prerequisites. Number of calculations givesdifferent levels of security and it depends on that they are so difficult to break, for example, we utilize Blowfish encryption calculation.

On the off chance that the cost required to break a calculation is more prominent than the estimation of the encoded information, then the calculation most likely is seen as protected. Be that as it may, present day top notch video encryption techniques have a few provisions and are imperilledto a broad aggression by master cryptanalyst. Comprehensive study and examination between these systems are anticipated to quantify the execution and to pick the better one for the proposed application. For a few applications measure of encryption might be the essential purpose of interest and for some different cases the protection will be crucial.

Differentattributes of a data security as such data confidentiality, data integrity, and authentication.

Here data is Encrypted by using the cryptography and exist as unreliable stream of the data to the third party by using a technique called substitution and transposition but the reality of the message is known to the hacker, where as in technique of Enigma the existence of the message is not evident. As defined by Caching, Enigma is the art and science of communicating in such a way that the presence of images cannot be detected.

Here the shared video must only be seen to a subset of users known as the authorized users. We shall attempt to make the secret shares verifiable using the concept of video encryption. The main idea is that a stream of images is encrypted using blowfish algorithm.

The public key cryptography algorithms are not going to assure the enigma while transforming the images. But the images can secure with the help symmetric key cryptography. In this type of cryptography same key is used for encoding and decoding purpose. Here symmetric calculation is divided into two stream cipher and block cipher. Stream cipher encode one piece of plain text at a time then block cipher which takes different bits(64 bits) and encrypt then as one unit as a whole.

The existing work done by using symmetric key techniques such as substitution method for Enigma. There are various techniques of Enigma but the images are mostly used to hide or embed the secret information. These types of techniques are known as image Enigma techniques. Image Enigma method can be categorized in to two groups i.e. the change of domain technique group and the spatial domain technique group.

AES is based on a design principle known as a substitution–permutation network, and is fast in both software and hardware.[9] Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Irondale which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Irondale *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

Advanced Encryption Standard, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. Brute force attack is the only effective attack known against this algorithm. AES encryption is fast and flexible. [8]

In the rest of the paper, organized as follows: In section II Literature survey, in section III methodology, in section IV Algorithm, in section V Implementation and in section VI conclusion.

II.LITERATURE SURVEY

In the Spatial domain method the intensity values of the pixels of the image are used to hide the information directly, while in the transform domain methods frequency domain of
Images which are previously transformed used to embed the information.When you consider the video,Promulgation is the arrangement of 1 to n numbers such that no numbers are repeated in the given video. Different methods for analysis of blowfish algorithm were proposed and found in [1].

As time passed AmmanJan tan[2] described a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish

Encryption And Decryption Using Blowfish Algorithm in Matlab was introduced by Pie Singh in 2013[3]. This paper is about encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms.

In [4] DineshandDr.P.SuveethaDhanaselvam showed howimages are considered with an aim to secure them during its storage and transmission. This is achieved using Blowfish Algorithm, a type of symmetric key cryptography. The two processes, encryption and decryption together form the cryptographic process. For ensuring security, the images are encrypted by the sender before transmitting them and are decrypted by the receiver after receiving them so that only the sender and the intended person can see the content in the image. Blowfish algorithm which uses a key of variable size up to 448 bits simply iterates the function 16 times (Feistel network).

The WDDL Logic implementation in Blowfish algorithm increases the speed from 570 Mbps to 840 Mbps. The simulation results and synthesis report proves better performance as well as security. The image processing is done using MATLAB and the Blowfish encryption;decryption is performed using the VHDL (Very Large Scale Integrated Circuits Hardware Description Language) platform Xilinx ISE 10.1.

In [6] image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. In this paper a Survey of Different Image Encryption and encryption techniques that are existing is given. It additionally focuses on the functionality of Image encryption and decryption techniques.

A process of finding and relating particular groups or communities is done in [6]. Here the communities which are not much detected by Yahoo or other search engines are first detected. These groups or communities though not familiar to all, but it may contain any valuable or reliable information in it. Hence detecting such communities will serve a purpose of finding information. Also these groups may become well-known in future.

In [10] we have a study of the two popular encryption algorithms: DES and Blowfish. We overviewed the base functions and analyzed the security for both algorithms. We also evaluated performance in execution speed based on different memory sizes and compared them. The experimental results show the relationship between function run speed and memory size.

With the high speed application growing of internet and wireless network, information security becomes significant to secure commerce secret and peace. Encryption algorithm helps in information security guarantee. In this paper, we evaluate the execution of two symmetric key encryption algorithms: AES and Blowfish which commonly used for network data encryption. In this paper, we analyzed encryption security, evaluated encryption speed and power consumption for both algorithms. Experimental results show that Blowfish algorithm runs faster than AES, while the power consumption remain the same. It is proved that the Blowfish encryption algorithm maybe more suitable for cryptographic software and wireless network application security.

In this paper, a video encryption technique is presented based on the two independent encryption procedures, which are used to protect different types of video. Compared with the single chaotic map scheme, the proposed algorithm will exhibit higher security. Due to the structure similar to the style of Feistel block cipher, the proposed algorithm can complete the encryption of two pixel blocks at one time, which is helpful for increasing data throughput. The security analysis shows that the method can resist many forms of cryptanalysis. It can be concluded from the results of good non-linear relation between plaintext and cipher text

III. METHODOLOGY

This paper discusses about the Blowfish Algorithm for Encryption and Optimization of Video. Here MPEG video of size 64-bit block of video-stream is encrypted and compressed and transmitted. The encryption takes place in two parts: Key Expansion and Feistal network encryption consisting of 16 iterations.Here the original video is converted into video streams. Each video stream is taken as an input.This input is resized into a 64-bit data. This data is divided into two 32-bit data. Encryption key is obtained by key expansion method, which has a key of variable length from 32-bit to 448-bits (14 bytes).

IV. ALGORITHM

Blowfish Algorithm

Blowfish algorithm is 64-bit symmetric block cipher, which varies from 23-bit to 448-bits (14 bytes) [1].

In our system this algorithm is used for encryption and decryption of the video. The encryption is done using one key and the same key is used for decryption of the video.

This algorithm has two parts.

- Key expansion
- Feistal network for encryption.

Key expansion converts a key varying from 32-bits to 448-bits into several sub key arrays of 4168-bits.

A 16-round Feistal network is used for video encryption. Each round has a key dependent permutation, a key and data substitution, which are operated by simple operations like XOR and addition operations on 32-bit data, where addition operations are the four indexed array data.

Sub Key generation

The sub keys must be generated before the data encryption or decryption. The process has 18 P-arrays of 32-bit boxes and four s-boxes of 32-bits. [2]

That is

P-array sub keys are

P1, P2, ……, P18

S-boxes have 256 entries each,

$SB_{1,0}$, $SB_{1,1}$, $SB_{1,2}$, $SB_{1,255}$.

$SB_{2,0}$, $SB_{2,1}$, $SB_{2,2}$, $SB_{2,255}$.

$SB_{3,0}$, $SB_{3,1}$, $SB_{3,2}$, $SB_{3,255}$.

$SB_{4,0}$, $SB_{4,1}$, $SB_{4,2}$, $SB_{4,255}$.

Procedure for encryption and decryption

The input is a 64-bit video, V

Divide V into two 32-bit parts: V_L, V_R

For x= 1 to 16

$V_{L=} V_L$ XOR Pi

$V_{R=} F(V_L)$ XOR V_R

Swap V_L, V_R

Swap V_L and V_R (undo the last swap)

$V_{R=} V_R$ XOR P17

$V_{L=} V_L$ XOR P18

Recombine V_L, V_R (See figure)

Function F (V_L):

Divide V_L into four 8-bit blocks, a, b, c, d [3].

$F(V_L)=((SB_{1,a} + SB_{2,b} \bmod 2^{32}) \text{ XOR } SB_{3,c}) + SB_{4,d} \bmod 2^{32}$)

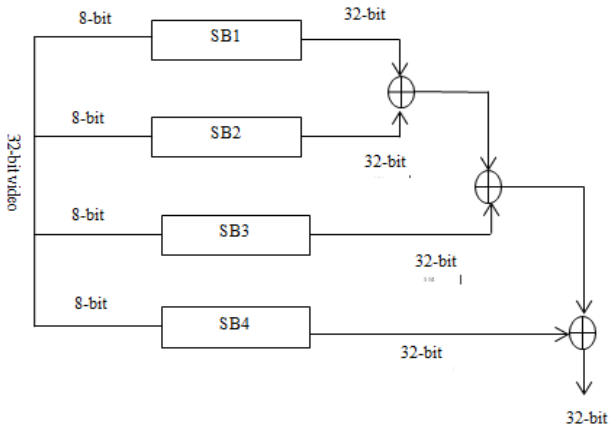

Figure 1: Function F.

V. IMPLIMENTAION

The Blowfish Algorithm takes less memory, less than 5K bytes Uses simple operations like XOR and additions, hence it is easy to implement. The hardware requirement is a 32-bit microprocessor at the rate of one byte for every 26 clock cycles. The key does not change very often hence more secure.

The goals of the system are

- Providing security to the confidential video.
- To assure the private multimedia data traded over the remote or wired system
- This system is much useful in the video recordings used as a part of administrations like video on interest, video conference learning. Also helpful in medicinal recordings, which might contain private data of a patient from the access by vindictive clients.

VI. CONCLUSION

This paper discusses about Encryption and Optimization of Video using Blowfish Algorithm. This Algorithm takes less memory, less than 5K bytes Uses simple operations like XOR and additions. Here Key Expansion and Feistal network encryption consisting of 16 iterations. This data is divided into two 32-bit data. Encryption key is obtained by key expansion method, which has a key of variable length from 32-bit to 448-bits (14 bytes).The key does not change very often hence more secure at the rate of one byte for every 26 clock cycles..

A more suitable algorithm using techniques like Dynamic Programming or Brute force algorithm to obtain the above results by considering the efficiency.

.

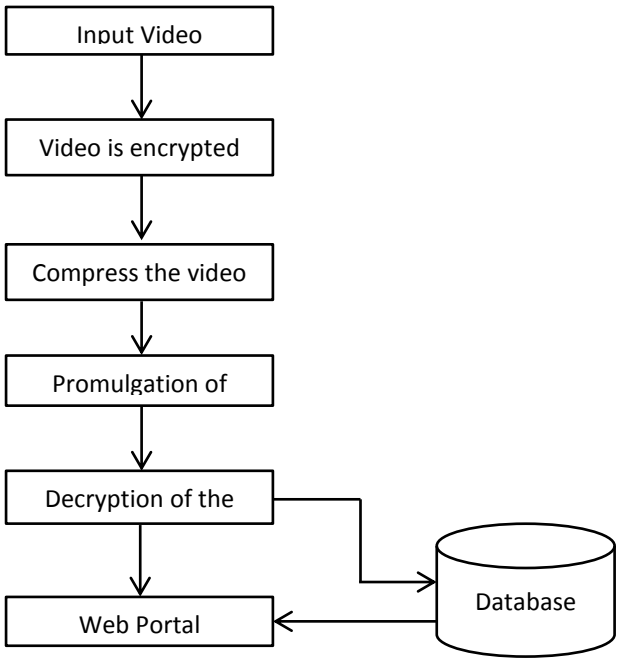

Figure 2: Architecture diagram

REFERENCES

[1] Vaibhav Poonia, Dr. Narendra Singh Yadav, *"Analysis of modified Blowfish Algorithm in different cases with various parameters",* International Conference on Advanced Computing and Communication Systems (ICACCS -2015), Jan. 05 – 07, 2015..

[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

[3] Pia Singh and Prof. Karamjeet Singh "*Image Encryption And Decryption Using Blowfish Algorithm In Matlab*", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013K.A.Sugeng,

[4] M.Dinesh And Dr.P.Suveetha Dhanaselvam," *Real Time Image Encryption And Decryption Using Blowfish Algorithm*", International Journal Of Emerging Technology In Computer Science & Electronics (Ijetcse) Issn: 0976-1353 Volume 22 Issue 2 – May 2016.

[5] Ankita Verma, Paramita Guha, Sunita Mishra,'' *Comparative Study Of Different Cryptographic Algorithms''*, International

Journal Of Emerging Trends & Technology In Computer Science (Ijettcs), Volume 5, Issue 2, March - April 2016.

[6] Pia Singh, Prof. Karamjeet Singh*," Image Encryption And Decryption Using Blowfish Algorithm In Matlab*", nternational Of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[7] S.G.K.D.N. Samaratunge, ―"*New EnigmaTechnique for Palette Based Images"*,In Second International Conference onIndustrial and InformationSystems, pp. 335-340, Aug. 8 – 11,2007.

[8] J. He, S. Tang and T. Wu, ―"*An Adaptive Image EnigmaBasedon Depth-Varying Embedding"*, In Congress on Image and SignalProcessing, vol. 5, pp. 660-663, 27-30 May 2008.

[9] S Roy and D.G. Akka, "*On complementary edge magic of certaingraphs"*, American Journal of Mathematics and Statistics 2012,2(3):22-26.

[10] Tingyuan Nie and Teng Zhang," *A Study of DES and Blowfish Encryption Algorithm*", IEEE, 2009.

Authors Profile

Dr. Dinesh S Pursed B.E., M.Techfrom Visvesvaraya Technological University, Belagaviand Ph.D from B.U. Bhopal, and currently working as Associate Professor and HOD-Department of Information Science and Engineering inBrindavan College of Engineering Bangalore.

*Mrs. Padmavathi H G*pursed Master of Technology from*University of Kuvempu Davanagare* in 2008and Bachelor of Engineering from University of Mysore in 1998 ,and currently working as Associate Professor in Department of Computer Science and Engineering in Brindavan College of Engineering Bangalore.

Mr. Madhu C.S pursed Master of Technology fromVisvesvaraya Technological University, Belagavi in 2011and Bachelor of Engineering fromVisvesvaraya Technological University, Belagavi in2008 , He is currently pursuing Ph.D in Visvesvaraya Technological University, Belagavi. and currently working as Assistant Professor in Department of Computer Science and Engineering in Brindavan College of Engineering Bangalore

Ms Divyashree H S Pursed Master of Technology from Visvesvaraya Technological University, Belagavi in 2013 and Bachelor of Engineering from Visvesvaraya Technological University, Belagavi in 2009, and currently working as Assistant Professor in Department of Computer Science and Engineering in Brindavan College of Engineering Bangalore

Mr. Bharath Raj D Pursed Master of Technology from Visvesvaraya Technological University, Belagavi in 2015 and Bachelor of Engineering from Visvesvaraya Technological University, Belagavi in 2011, and currently working as Assistant Professor in Department of Information Science and Engineering in Brindavan College of Engineering Bangalore

