International Journal of Research in Engineering, Science and Management
Volume-2, Issue-8, August-2019
www.ijresm.com | ISSN (Online): 2581-5792

RC5 Algorithm for Video

Anuj Sharma[1], Harsh Sharma[2]
[1]*Student, Dept. of Electronics & Telecommunication, Thakur College of Engg. & Technology, Mumbai, India*
[2]*Student, Dept. of Electronics & Telecommunication, Universal College of Engg., Thane, Maharashtra, India*

***Abstract*: Multimedia data security is becoming important with the continuous increase of digital communications on internet. With the 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. The encryption algorithms developed to secure text data are not suitable for multimedia application because of the large data size and real time constraint. Therefore, there is a great demand for secured data storage and transmission techniques. Information security has traditionally been ensured with data encryption and authentication techniques. The secrecy of communication is maintained by secret key exchange. In effect the strength of the algorithm depends solely on the length of the key. The presented work aims at secure video transmission using randomness in encryption algorithm, thereby creating more confusion to obtain the original data today. The proposed work finds its application in medical imaging systems, military image database communication and confidential video conferencing, and similar such application. The results are obtained through the use of MATLAB.**

***Keywords*: Key; Cryptograph; Encryption; Video encryption.**

1. Introduction

In the current era, the communication through multimedia components is on its peak. The data like text, images, video and audio is communicated through network [1]. The communication network is like a platform for malicious users and other intruders who try to intercept or even harm the information that is communicated via the network. To protect the information from being leaked, it is necessary to send it in a form which is unreadable. For providing such security, cryptography comes into play. Cryptography is the art or science of secrecy. It is about communicating securely through insecure channels. It not only protects the data from alterations and theft, but also provides user authentication. There are three types of cryptographic schemes which have been discussed below. The initial data or normal text is referred to as plaintext.

When this plain text is encrypted, it is called as cipher text. This cipher text, when decrypted will again turn into usable plaintext.

Following are some of the goals of security [1], [2].

- Authentication: The process of proving one's identity.
- Confidentiality: It ensures that the message can only be read by the intended receiver.
- Integrity: It assures the receiver that the message that has been received, unaltered.
- Non-repudiation: The sender cannot deny having sent the message and also the receiver cannot deny having received the message.

Fig. 1. Pyramid view of Security

The algorithms in cryptography are broadly classified into the two classes, Symmetric and Asymmetric algorithm.

A. Symmetric Key Cryptography

In this scheme, the keys used for encryption and for decryption are the same. The secret key should be known to both the sender as well as the receiver. The difficulty in this approach arises in the distribution of the key. It is generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time. A block cipher encrypts one block of data at a time. It can be in Electronic Code Book mode (ECB), Cipher Block Chaining mode (CBC), Output Feedback mode (OFB).

Various algorithms which fall under the category of Symmetric key cryptography are:RC2, RC4, RC5, RC6, AES, DES, 3DES, Blowfish, Two fish.

B. Asymmetric Key Cryptography

It makes use of a pair of keys. One key is used for encryption and another is used for decryption. The decryption key is kept secret which is called as “private key” or “secret key”, while “public key” is send to all for encrypting messages. Examples are RSA, DSA, and ELGAMALAES (Advanced Encryption Standard), etc.

2. RC5 algorithm

RC5 is a 32/64/128-bit block cipher developed in 1994. It was designed by Ronald Rivest for RSA Data Security (now RSA Security) in December of 1994. It is a symmetric block cipher having a variable number of rounds, word size and a

secret key [3]. It uses data-dependent operations heavily. It is a simple algorithm which has a low memory requirement. It is suitable for hardware or software. It is fast and also provides security if suitable parameters are chosen. Due to the data-dependent rotations, differential cryptanalysis and linear cryptanalysis is not possible. The key used is strong if it is long. However, if the key size is short, then the algorithm is weak.

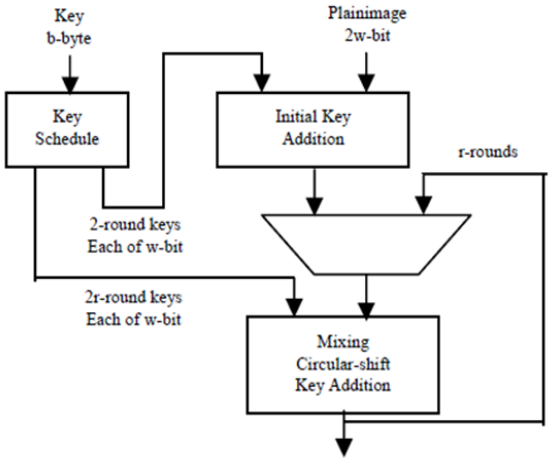

Fig. 2. RC5 Algorithm

It uses a key of selectable length b (0, 1, 2, ..., 255) byte. The algorithm is organized as a set of iterations called rounds r that takes values in the range (0, 1, 2, ..., 255) as illustrated in above figure [4].

An expanded key array is created out from the original key by means of a key schedule. The expanded key array is used with both encryption/decryption routines and its length is dependent on the number of rounds. The operations performed on the data blocks include bitwise exclusive-OR of words, data-dependent rotations by means of circular left and right rotations and Two's complement addition/subtraction of words, which is modulo- 2^w addition/subtraction, where w is the word size in bits. They always affect a complete 16, 32 or 64-bit data block at a time.

3. Proposed system

Videos are transferred through various types of computer network. To secure video communication different encryption methodologies are used. We have proposed a system for videos encryption, using RC5 Algorithm to safely exchange highly confidential videos. Also, to maintain a balance between security and computational time, the proposed algorithm shuffles the video frames along with the audio, and then RC5 is used to selectively encrypt the sensitive video code word. In the encryption system the block of video is firstly divided into frames, then these blocks of frames are encrypted using block ciphering technique such as RC5. Using this approach unauthorized viewing of the video file can be prevented and hence this algorithm provides a high level of security.

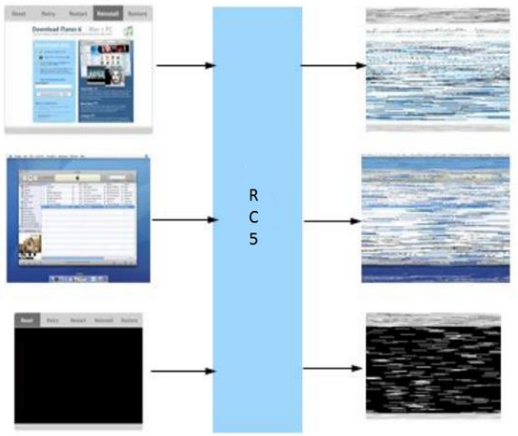

Fig. 3. Encryption Block

4. Methodology

There are two inputs to the encryption function, which are the plain image to be encrypted and the expanded secret key. For RC5 image encryption, the image header is extracted from the image to be encrypted and the image data stream is divided into blocks of 64-bit length [11]. The first 64-bit block of image is entered as the plain image to the encryption function of RC5. The second input the RC5 encryption algorithm is the expanded secret key that is derived from the user-supplied secret key by the key schedule. Then, the next 64-bit plain image block follows it, and so on with the scan path shown in Figure. 4 until the end of the image data bit stream.

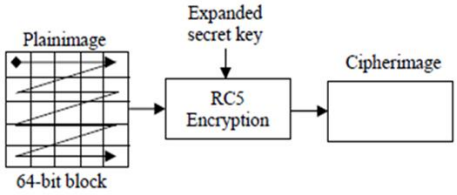

Fig. 4. Image Encryption using RC5

In the decryption process, the encrypted image (cipher image) is also divided into 64-bit blocks. The 64-bit cipher image is entered to RC5 decryption algorithm and the same expanded secret key is used to decrypt the cipher image but the expanded secret key is applied in a reverse manner. Then the next 64-bit cipher image block follows it, and so on with the same scan path as shown in Figure 5.

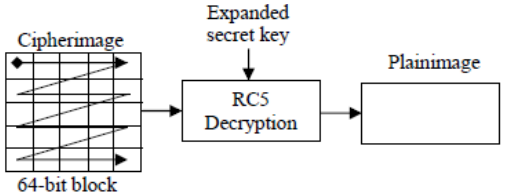

Fig. 5. Image Decryption using RC5

A. Video to image conversion

Using the algorithm directly on the video files will be a very complex computation so to achieve this task very easily and

simply the video files should be first converted into frames and then after converting it into frames after an interval of just suppose 0.2 sec the image will be formed by using a for loop and 'imwrite' command from o to 255 i.e. in both direction (rows and columns) as the video is a 2D representation of 3D object and image is also 2D representation.

B. RGB to gray conversion

Colour image contains a large number of pixel value as compared to grayscale image so it would be easier to operate or perform hash functions on grayscale image so convert the image into gray image by using a for loop as used above. The coloured image is the converted into greyscale image this is because the luminance of a pixel value of a grayscale image ranges from 0 to 255 [8]. The conversion of a colour image into grayscale image is converting the rgb values(24bit) into grayscale value (8bit) for simplicity [4]. By converting the colour image or Rgb into gray we enter into a domain which is much easy for processing and computation complexity reduces as there are less information present.

C. Append Padding Bits

First calculate the length of the message but here the message is a video file which is converted into image frames or to be precise grayscale image's which is of 8 bit so first convert it into 8 parts from MSB to LSB [2]. After that message is padded with a 1 and as many 0's as necessary to bring the message length to 64 bits fewer than an even multiple of 512 [2]. To make the length congruent to 448 modulo 512.

D. Append Length

The data is then a fixed length of 448 bits which is 64 less than 512. Then 64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message [2]. The output of the first two steps is a message that is an integer multiple of 512 bits in length in this case image of 512 bits block [2].

E. Key Expansion

This routine expands the user's secret key K to fill the expanded key array S, S resembles an array of t=2(r+1) random binary words determined by K. It uses two word-sized binary constants Pw and Qw. They are defined as,

(1) Pw = odd((e-2)2w)
(2) Ow = odd((∅-1)2w)
Where
e= 2.718281828459…….. (base of natural logarithms)
∅= 1.618033988749…..(golden ratio)
The three steps of key expansion are as follows:

1) Converting the secret from bytes to words

The expansion process first copy the secret key K[0…b-1] into an array L[0…c-1] of c=[b/u] words, where u=[w/8] is the number of bytes/word.

2) Initializing the array S

The second process is to initialize array S to a pseudo random bit pattern using arithmetic progression by constant values Pw and Qw.

S[0]=Pw;
For i=1 to t-1 do
S[i]=S[i-1]+Qw;

F. Encryption

The input block is given in two w-bit registers A and B. Key expansion has been already performed, so that array S[0…t-1] has been computed.

A=A+ S[0];
B= B+ S[1];
For i=1 to r do
A= ((AB) <<< B) + S[2*i];
B= ((BA) <<< A) + S[2*i +1];
The decryption is the inverse process of encryption routine.

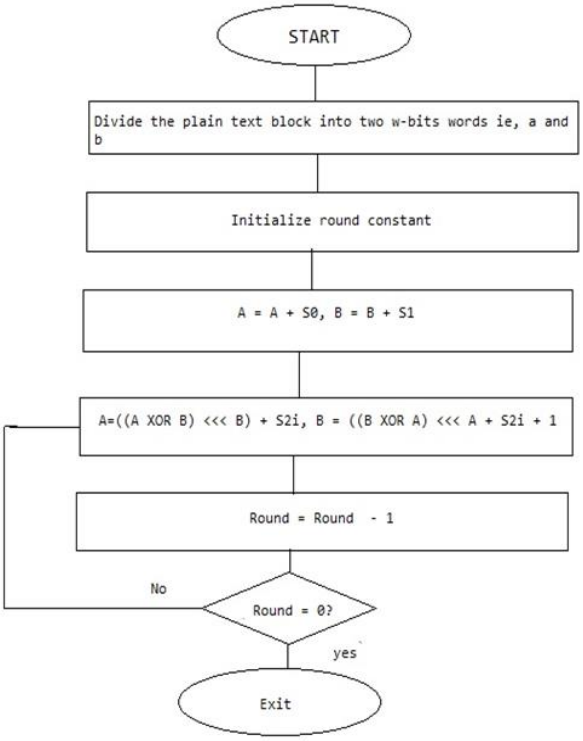

Fig. 6. Encryption flow diagram

5. Result

By performing this algorithm on the video file we are expecting the following result that is the video file will be compressed and it will ask for finger print for opening the data file.

6. Conclusion

Encryption on the multimedia is essential in both commercial broadcasting and peer to- peer communication. In this project we have successful implemented video encryption as well as decryption. With the combination of MATLAB code, a unique solution for video encryption is provided here. This encryption uses variable length of key. Firstly, video signals or motion signal is converted into block of frames. Further these frames

are individually sent for encryption. The proposed methodology is applied for ensuring the personal privacy in the context of Digital Rights Management systems. Wherein Only the authorized person that possess the key can decrypt the entire encrypted video. Also with the added advantage of this algorithm being, a fast symmetric block cipher makes it suitable for hardware or software implementations. A novel feature of RC5 is the heavy use of data-dependent rotations which makes it more secure as compared to other algorithms which are currently present.

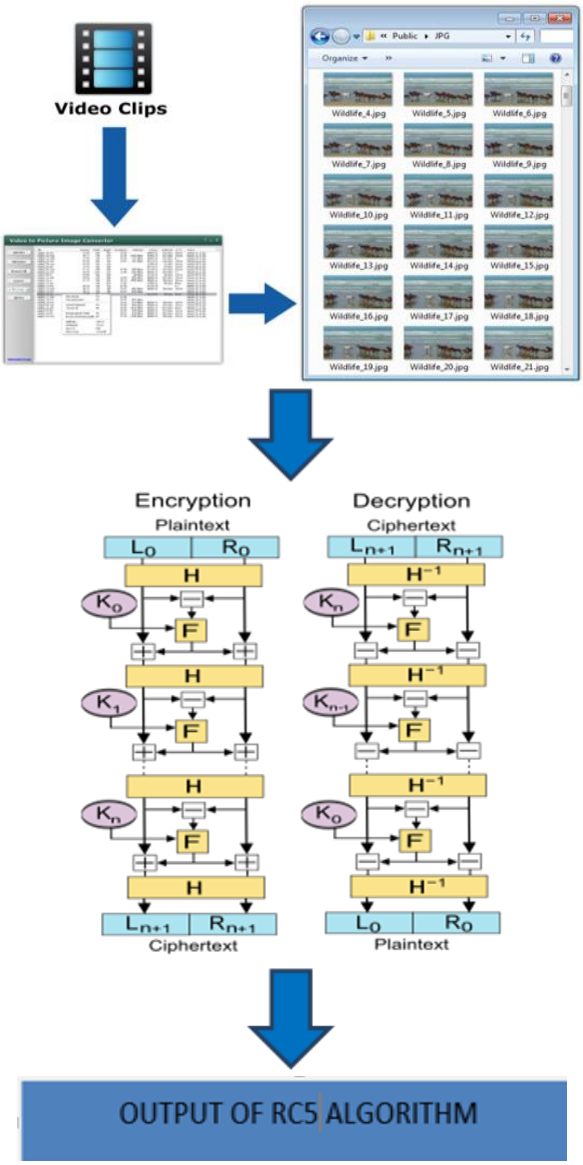

Fig. 7. Flow diagram for RC5 Algorithm

7. Future scope

1. The proposed system can be extended to standard video coding systems such as those using MPEG and other video formats. All the existing costly encryption products will have no use in future if the video encryption also invented with royalty free open source software. Therefore, it will be the most flexible and cheaper solution.
2. Tunable selective encryption algorithms could be developed for balancing computational cost and security.

References

[1] Atul Kahate, Cryptography and Network Security, (Second Edition 2008)
[2] International Journal of Information & Computation Technology, vol. 4, no. 17, pp. 1831-1838, 2014.
[3] W. Stallings, "Cryptography and Network Security: Principles and Practice," Prentice-Hall, New Jersey, 1999.
[4] Shujun Li and Xuan Zheng, "On the security of an image encryption method," in Proc. IEEE Int. Conference on Image Processing (ICIP'2002), vol. 2, pp. 925-928, 2002.
[5] Shujun Li and Xuan Zheng, "Cryptanalysis of a chaotic image encryption method," in Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2002), vol. 2, pages 708-711, 2002.
[6] Ronald L. Rivest, "RC5 Encryption Algorithm," Dr Dobbs Journal, vol. 226, pp. 146-148, Jan. 1995.
[7] Bruce Schneier, "Applied Cryptography – Protocols, algorithms, and source code in C," John Wiley & Sons, Inc., New York, second edition, 1996.
[8] Shi, S. Y. Wang, and B. Bhargava, "MPEG Video Encryption in Real-time using Secret Key Cryptography," in Proceedings of the International Conference on Parallel and Distributed Processing Algorithms and Applications,1999.
[9] Wu C-P, Kuo C-CJ, "Design of integrated multimedia compression and encryption systems". IEEE transaction on Multimedia (7)(5):828-39; October 2005.
[10] Narsimha Raju, Ganugula Umadevi, Kannan Srinathan, C.V. Jawahar, "Fast and Secure Real-Time Video Encryption" in Sixth Indian Conference on Computer Vision, Graphics & Image Processing 2008:257.