MJRET

Open Access

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 - 6953

SECURE STORAGE OF VIDEO BY ENCRYPTION USING 4 OUT OF 8 CODES AND SCANNING TECHNIQUES

Pratik Vishnu Sawant

First Year M.Tech, Software Engineering
Veermata Jijabai Technological Institute,
Mumbai, India

Abstract: *Hiding data is essential for everyone whether it is an organization or an individual by considering the data theft and privacy violation incidences. Data can be in any form i.e. textual data or visual data. Visual data mainly consists of images and video files. Video files may contain some important or confidential records which can create huge amount of loss if leaked or made available publically. Hence, securing video files for storage is very much important. The paper presents technique for efficient encryption and decryption of video files. For encryption, paper uses combination of previously defined Four out of Eight codes and Scanning Techniques presented in the paper. Paper also presents decryption methodology which uses authentication and authorization to ensure that the videos which are encrypted by the system are been accessed by the legitimate user after decryption.*

Keywords*: Encryption, Decryption, authentication, authorization, data theft, data hiding, security, video files, four out of eight, scanning techniques*

1. INTRODUCTION

In modern days, we are using lots of media files especially video files. There is possibility that video files may contain some sensitive data which is not intended except trusted user. These video files may be the recordings of some organizations internal structure, some patented process or recording of some secret conferences or may be proof of some criminal case.

If such sensitive information is leaked, it may cause harm to related organization. Hence, this project focuses on the file system, especially video files to hide them from the unauthorized users by encrypting them to secured level.

The project follows traditional approach of key, but the actual encryption is done by internally generated key which is derived from the actual key and unknown to the external world.
The project is focusing on encryption processing, but it will also decrypt the stored video file by authenticating the legitimate user on the basis of key produced. Hence, Decryption is also the part of project along with Encryption as primary focus. And authentication module have also been introduced without which decryption is not possible. Hence, the basic idea will revolve around four out of eight [1] method and scanning techniques [2] for encryption and decryption of video.

2. LITERATURE REVIEW

Video Encryption[9] is basically divided into four categories[3]:

2.1 Completely Layered Encryption

Video encrypted in this type of encryption uses traditional algorithms like RSA, DES and AES. This type of encryption leads to heavy computations and hence has heavy resource utilization.

2.2 Encryption Using Permutation

This encryption style contains scrambling of video content using permutation algorithm.

2.3 Selective Encryption

Only particular video contents will be encrypted here. Hence, it is low on computational time and resource utilization. Proposed system is example of selective encryption technique.

1.4 Perceptual Encryption

It is weak style of encrypting video since videos are perceptible. We have to continuously monitor audio and video quality.

Further, we can have different cryptography models based on what type of keys is used for encryption and decryption.

1) Symmetric key encryption models[4][5]
2) Asymmetric key encryption models
3) Hash functions (Mathematical) models

The proposed encryption technique uses Symmetric Key encryption model. Symmetric key, as name suggests, uses same key for encryption[8] and decryption[8] purpose. Examples of

symmetric key encryption algorithms can be DES[4][5][7] and AES[4][5][6]. This model uses either stream cipher or block cipher for the encryption. Stream cipher ensures encryption of element one by one whereas block cipher refers to encryption of block of data at a time.

3. FOUR OUT OF EIGHT CODES

Serial Number	Binary	Hexadecimal	Decimal	Alpha Numeric
1	00110011	33	51	A, a
2	00110101	35	53	B, b
3	00110110	36	54	C, c
4	00111001	39	57	D, d
5	00111010	3A	58	E, e
6	00111100	3C	60	F, f
7	01010011	53	83	G, g
8	01010101	55	85	H, h
9	01010110	56	86	I, i
10	01011001	59	89	J, j
11	01011010	5A	90	K, k
12	01011100	5C	92	L, l
13	01100011	63	999	M, m
14	01100101	65	101	N, n
15	01100110	66	102	O, o
16	01101001	69	105	P, p
17	01101010	6A	106	Q, q
18	01101100	6C	108	R, r
19	10010011	93	147	S, s
20	10010101	95	149	T, t
21	10010110	96	150	U, u
22	10011001	99	153	V, v
23	10011010	9A	154	W, w
24	10011100	9C	156	X, x
25	10100011	A3	163	Y, y
26	10100101	A5	165	Z, z
27	10100110	A6	166	0
28	10101001	A9	169	1
29	10101010	AA	170	2
30	10101100	AC	172	3
31	11000011	C3	195	4
32	11000101	C5	197	5
33	11000110	C6	198	6
34	11001001	C9	201	7
35	11001010	CA	202	8
36	11001100	CC	204	9

Table 1: Four Out of Eight Codes [1]

Four out of Eight codes are basically binary 8 bit binary numbers having four 1's and four 0's i.e. first 4 bits have two 1's and two 0's and similarly in next 4 bits. This table will be useful in generating encryption key.

4. SCANNING TECHNIQUES

Every Scanning Technique is a basic flow of how we are going to read a source video file and how it will be written after encryption. Writing of the encrypted file is kept untouched and concentration is shifted only on reading patterns. Some of the reading patterns are as shown in the following figures.

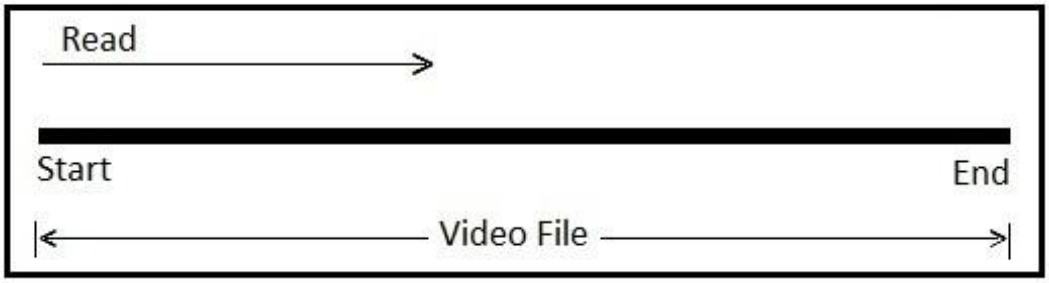

Fig.1 Forward

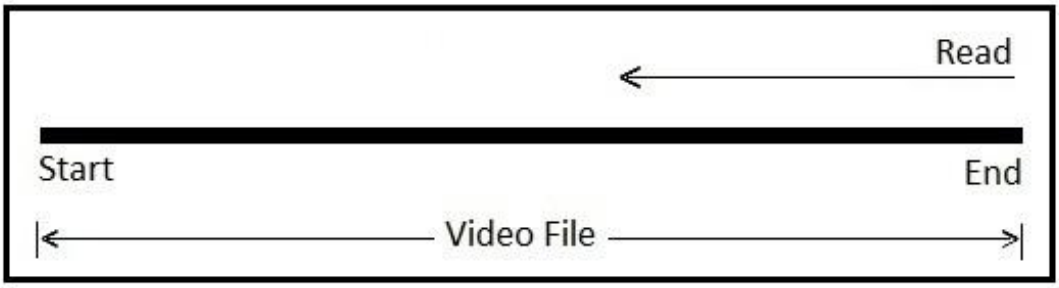

Fig.2 Backward

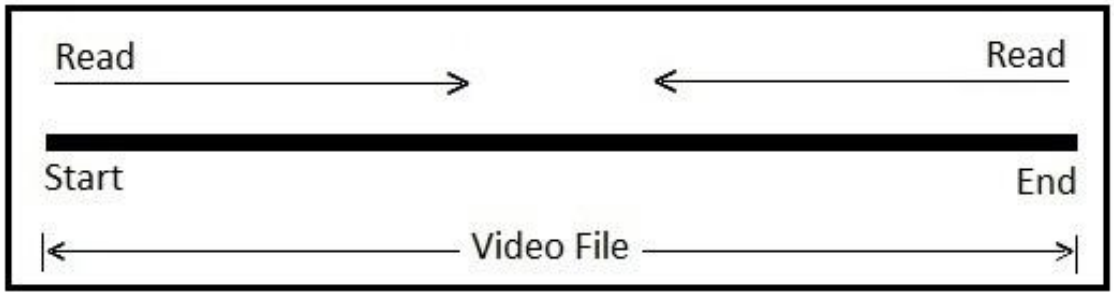

Fig. 3 Concurrent from Ends

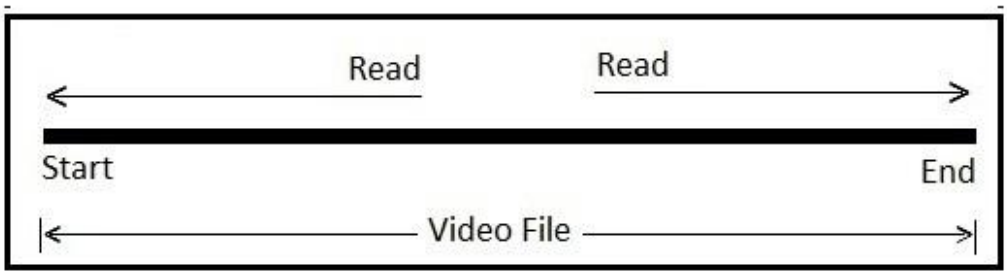

Fig.4 Concurrent toward Ends

These are some example patterns. Here it is possible to skip some data from getting encrypted to increase speed of execution.

5. ENCRYPTION

As shown in fig. encryption process, user key gets converted into encryption key by processing in the 4 out of 8 method which is based on 4 out of 8 table mentioned above. This encryption key, pattern and source video is combined at encryption process to process out desired encrypted video.

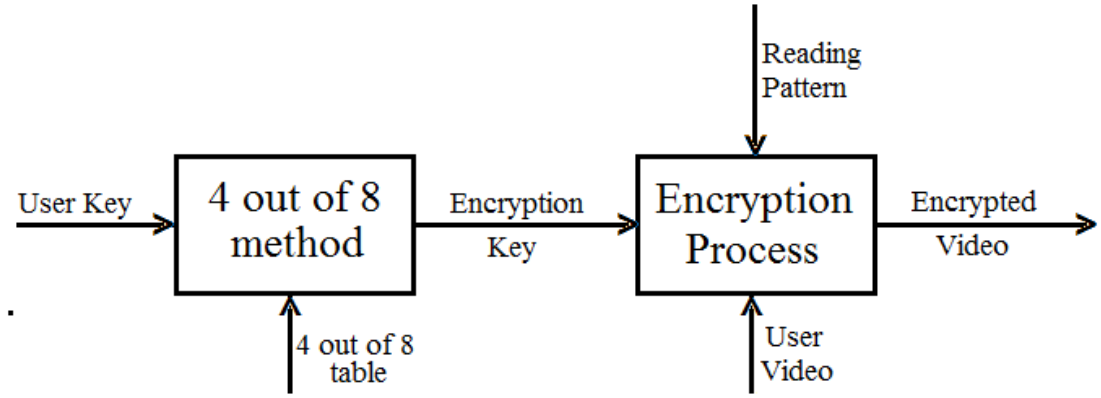

Fig.5 Encryption Process

Encryption Algorithm:

1. *Fetch Encryption Key from 4 out of 8 modules.*
2. *Generate name for new encrypted file.*
3. *Create new file with generated name.*
4. *Write some elements of key at predefined positions.*
5. *Fetch video file byte by byte from address specified.*
6. *Fetch Read Pattern.*
7. *Decide interval of encryption 'n'.*
8. *For each byte do 8^{th} and 9^{th} step till end of file.*
9. *EXOR every n^{th} element of file.*
10. *Write every byte in created file.*

6. DECRYPTION

As shown in fig. decryption process, user key gets converted into decryption key by processing in the 4 out of 8 method which is based on 4 out of 8 table mentioned above. This decryption key, pattern and source video is combined at decryption process to process out desired decrypted video. But, authentication has important role here, hence authentication module is used before start of the decryption process.

Authenticator and Pattern Decider will read the control information embedded by the encryption process and will verify it with the current user key provided. The encrypted file will hold the part of encryption key but not the whole key hence, it will be difficult to decrypt the fetched encrypted file even if part of key remains present in it. And only authenticator may verify it.

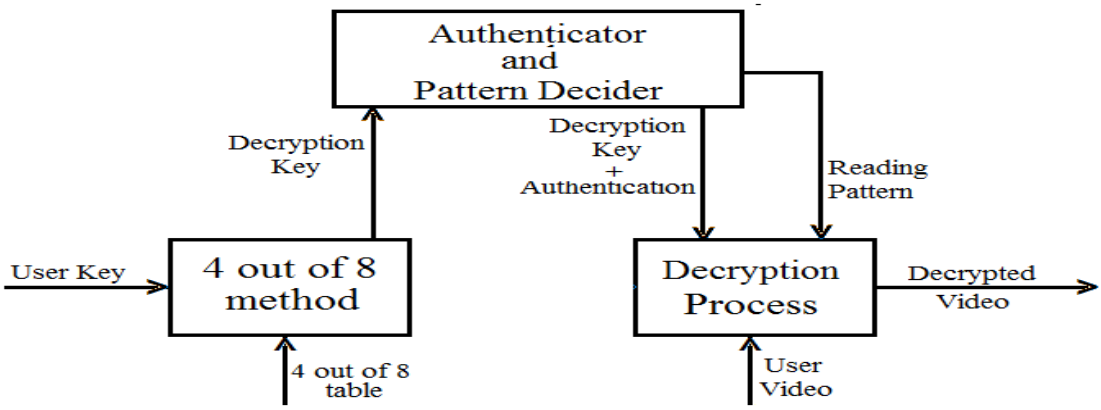

Fig.6 Decryption Process

Decryption Algorithm:

1. *Get user key*
2. *Generate decryption key.*
3. *Verify user key with partial key embedded in encrypted file.*
4. *Only if match found, perform step 4. Else terminate.*
5. *Fetch name for decrypted file.*
6. *Create new file to store decrypted data.*
7. *Fetch pattern.*
8. *Fetch interval of encryption 'n'.*
9. *Start decryption by repeating steps 10 and 11 till end of file.*
10. *EXOR every n^{th} element of encrypted file.*
11. *Write every byte.*

7. RESULTS

The proposed system will encrypt the given file and write some control information on it for future decryption process. At the decryption end, system will first authenticate whether this

video is encrypted or not and simultaneously will be checking for the user is authorized or not to view this file. The legitimate requests will be accepted and file will be decrypted, else system will show an error since it is unable to process the request. It might be possible, that for closely correct keys i.e. part of user key written inside encrypted file is correct and other part is incorrect then system may fail by executing decryption module, but unauthorized user will never able to get actual video file since, decryption is fully dependent on decryption key which is function of user key.

According to performance parameters of video encryption,

1. **Security level**
   Security level will be high in the proposed system since the data is changed at byte level, hence, the video will be in completely disturbed format which cannot be opened with any video player unlike other algorithms working on frames of video. Hence, it is better than perceptual encryption system.
2. **Speed**
   Speed of encryption will be based on actual size of video file on disk and not on the frames and density of frames in the video. Time complexity of the algorithm, which is combined feature of read pattern and encryption interval can be defined in worst case as O(n) where n is number of bytes. This is better than other video encryption algorithms working on frames of video.
3. **Video Size**
   Size of video remains unchanged with this algorithm. Which leads to no data loss and quality of video retains even after number of encryption and decryption cycles.
4. **Encryption Ratio**
   Encryption ration is function of encryption interval which changes dynamically for every video encryption. Ideally the encryption ratio should be from 20% to 50% for faster performance needs and from 50% to 100% where security is more important than resource and time utilization.

8. CONCLUSION & FUTURE SCOPE

The system proposed here is an efficient technique for encryption and decryption of video files. It gives full customization and freedom for improvements as all parameters for encryption can hold different values at different time and at different application projects. The system is reliable since it will not decrypt the file properly without correct user key which prevents it from unauthorized access.

As system is fast, it can be implemented in video players which wants to save video player dependent videos and decrypt the video in real time i.e. at the time of rendering.

REFERENCES

[1]. Panduranga H.T, Naveen Kumar S.K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images"

[2]. Chao Shen Chen and Rong Jian Chen, "Image encryption and decryption using SCAN methodology," Proc. PDCAT, 2006.

[3]. Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas and Aniket More "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study"

[4]. Milind Mathur.and Ayush Kesarwani "Comparison Between DES , 3DES ,RC2 , RC6, BLOWFISH And AES", Proceedings of National Conference on New Horizons, university of Oklahoma, , ISBN 978-93-82338-79-6,2013.

[5]. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[6]. Douglas Selent, "Advanced Encryption Standard", InSight : RIVIER ACADEMIC JOURNAL, VOLUME 6, NUMBER 2, FALL 2010

[7]. Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[8]. H. Lee Kwang, Department of Electrical Engineering & Computer Science, KAIST, "Chap 2. Basic Encryption and Decryption"