A Novel Approach of Digital Video Encryption

Mayank Arya Chandra
USIT,GGS IP University
Delhi India

Ravindra Purwar,
USIT,GGS IP University
Delhi India

Navin Rajpal
USIT,GGS IP University
Delhi India

ABSTRACT

In the recent years with the development of internet technologies, video technologies have been broadly used in TV, communication and multimedia, So security is required on video data. Although much video encryption technique has been develop but not give so much efficiency in terms of encryption and decryption process. However, they are more complex to implement as a system and are difficult to be applied in a widespread manner. Here we propose a new novel scheme for digital video encryption. In this paper we give a method to generate an encrypted video by encrypted Video-frame. Based on novel secure video scheme, an effective and generalized scheme of video encryption. It is a matrix computation scheme which uses a concept of Video-frame and xor(⊕) operation. This paper proves that proposed scheme is able to fully encrypt the video frame and have a better performance that can be measured by different Parameters. Further we can extend our approach into a digital video stenography.

General Terms

Video Encryption, Formation Algorithm, Deformation Algorithm

Keywords

video encryption, video-frame, security, sorting, formation algorithm**.**

1. INTRODUCTION

Rapid growth in internet and video technology we need to provide the security to the video data as well as authentication. During recent years with the development of video technologies have been broadly used in TV, communication and multimedia, video security has been required. now days video encryption is one of the most important field of information security.

In every section of the industry, large amount of data, images, videos with some confidential information are generated and stored and transmitted over the network. In addition ,medical images with a patient 's record s may be shared among the doctors of different department of hospital for different clinical purposes. these image and video may contain private information. So protection of, such type of multimedia data in life time, is an issue. Hence encryptions are needed to protect the confidential data.

Several interesting approaches for video encryption have been developed encryption of video and other multimedia data through conventional cryptography such as DES[1], AES[2], RSA[3] are not suitable for various differences of text data and multimedia data. Other types of encryption technique also use like as Scrambling of pixel position [4].

Naïve algorithm is the most straight-forward method to encrypt every byte in the whole Moving Picture Experts Group (MPEG) [14], video stream using standard encryption schemes such as DES or AES. The concept behind the Naïve algorithm is to treat the MPEG bit stream as text data and does not use any of the special structure [15][16][17]. In the Zig-Zag permutation approach [18], 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).

Basically, there are two methods for encryption of an image as well as video. One approach is Full Encryption Approaches. In which encryption process apply on the entire video bit stream. Second is a Selective Encryption Approaches that perform encryption only a certain or a specific part while other part remain unencrypted [5]. Selective encryption algorithms were proposed [38][39][40]. These methods encrypt a selected portion of the video data using text based encryption algorithms. This decreases encryption time. Another category of algorithms is based on scramble (permutation) only methods, where the DCT coefficients are permuted to provide confusion. However, in most of these methods, computational efficiency comes at the cost of security.

In the field of neural network, chaotic theory is very popular for encryption and decryption.[6][7][8][9][10], main advantage of chaotic network is that it is low cost, which is suitable to large amount of data.

Now In this paper we propose a new efficient scheme for video encryption using key image which is use for full encryption process. This paper consists following sections: In section Ist background encryption algorithm. Section 2nd Proposed Scheme, 3rd section describes the Formation and Deformation algorithms, 4th section describes the experimental results, 5th section describes the conclusion and 6th section references.

2. PROPOSED SCHEME

In this paper we have proposed a new scheme for video encryption which based on encryption of I-frame (video frame).Here we have taken an idea from matrix calculation for generating the encrypted I-frame. In this method, we collect the all video frame then take frame one by one form it and select a key Image as key frame for encryption and decryption process, so this key image is send through secure channel. Other frame encrypted by following algorithm . after applying the encryption algorithm we combine all frame, make video which is in encrypted form, send it from simple channel.

Let V be a video sequence consisting of m frames denoted by I1, I2, . . . Im. Furthermore, we assume that each frame has a dimension of w ×h and up to 2n different pixel values (colors). Finally, let α_i denote any sorting permutation of Ii , and α(Ii) the image with sorted pixels from Ii . For a given frame I there are a large number of sorting permutations for I. By a sorting permutation of I we mean a unique sorting permutation α that any two distant parties can compute solely by knowing I, which is the case when the parties utilize the same computational method. For example, the communicating parties can agree on always choosing the lexicographically smallest sorting permutation of frame I. A more efficient method for generating a sorting permutation relies on using a standard sorting algorithm such as quicksort , heapsort . Overall encryption procedure defines in the deformation algorithm. Basically In this system video stream assumes as a collection of still images, get these images refers as an I-frame. First frame do not encrypted, it is transmitted through a secure channel. Select second frame performing the xor(⊕) operation with second key image and then xor(⊕) with sorted value of first frame. The output of the above process xor(⊕) with sorted form of the first key frame. now this is the final encrypted image. then make the digital video through these encrypted images and send this video through simple channel. But key image transmitted through secure channel. At the receiver side reverse process is applied.

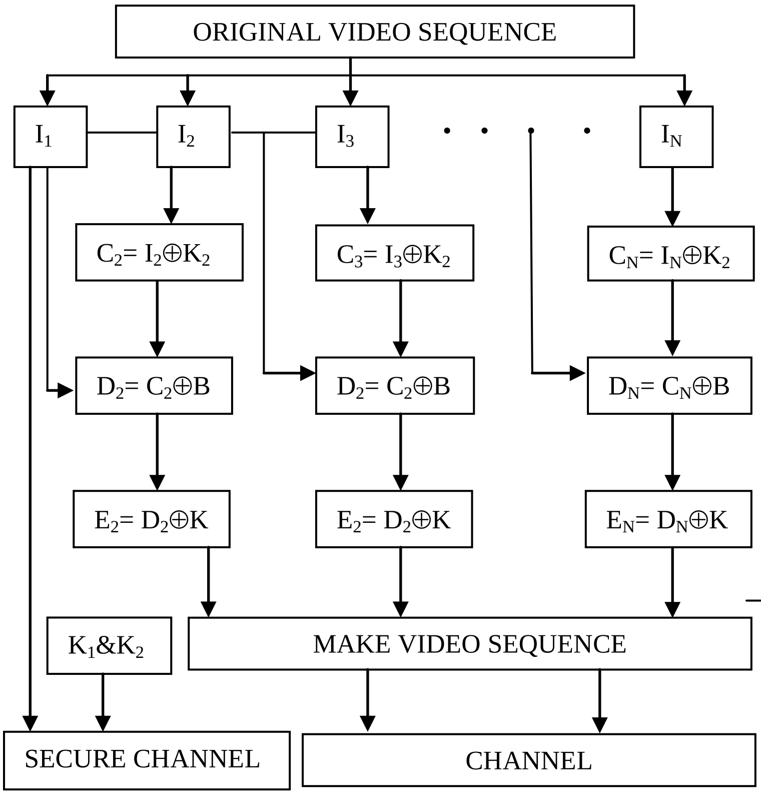


Figure 1. Video Encryption System

Given figure show how the encryption/decryption process applied. Figure number (1) Represent the encryption System Figure number (2) represent the decryption procedure.

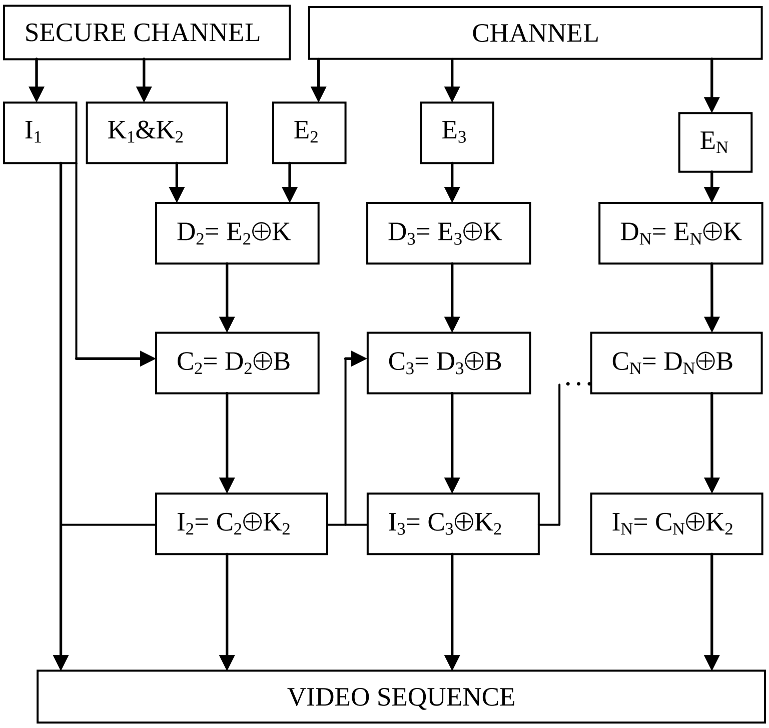


Figure 2. Video Decryption System

3. PROPOSED ALGORITHM

3.1 Deformation Algorithm

The following is a proposed deformation algorithm for encryption.

Definition:

ν_n: Video stream , I_n: Video Frames

n= {0,1,2………………}

K_1, K_2: Key Image

α: Sorting function

Step1 Choose any video stream V.

Step2 Compute all frame of video stream V (I_1, I_2, I_3…..I_n).

Step3 $A_n = I_n$, Where n= 2, 3 …n.

Step4 $B = \alpha(\text{Rand}(I_n))$ Where n= 1,2, 3 …n-1.

Step5 $K = \alpha(K_1)$

Step6 $C_n = (A_n \oplus K_2)$

$D_n = (C_n \oplus B)$

$E_n = (D_n \oplus K)$

Step6 Repeat step 3rd ,4 th & 5th step for all frames.

Step7 Construct video from Encrypted frame.

Step8 Transmit this video through simple channel.

Step9 Transmit Key frame, Random frame sequence and I_1 through Secure channel

3.2 FORMATION ALGORITHM

The following is a proposed deformation algorithm for decryption.

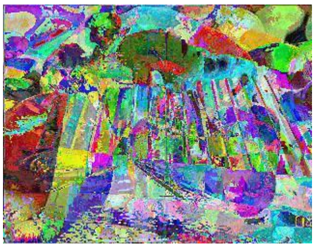
```
Step 1   Receive Video Stream data and first frame, Random sequence no and Key image.
Step 2   Compute all frame of video.
Step 3   $K = \alpha(K_1)$
Step 4   $B_n = \alpha(I_n)$ Where n= 1,2, 3 …n-1
Step 5   $D_n = (E_n \oplus K)$
         $C_n = (D_n \oplus B_{n-1})$
         $I_n = (C_n \oplus K_2)$
Step 6   Repeat step 4 th , 5th for all frame.
Step 7 Construct original video through I-fame
```

4. EXPERIMENATAL RESULT

This section of the paper contains the result analysis of the proposed encryption scheme. The formation algorithm has been successfully implemented in 4 different videos. Several simulation results are provided to show the performance of the algorithms for video encryption.

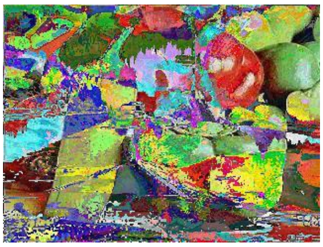
4.1 Video data

1) Xylophone Video



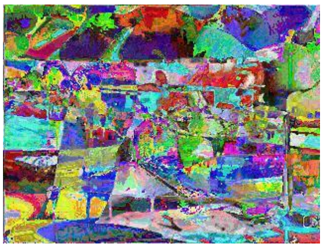
1. Before Encryption 2. After Encryption

2) Shaky_car.avi



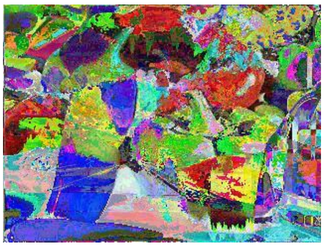
1. Before Encryption 2. After Encryption

3) Vipmosaicking.avi



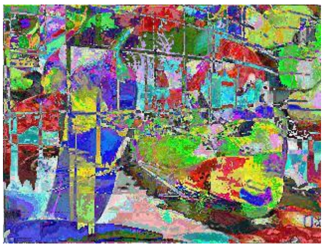
1. Before Encryption 2. After Encryption

4) Rhinos.avi



1. Before Encryption 2. After Encryption

5) Vipsnowydays.avi



1. Before Encryption 2. After Encryption

4.2 RESULT ANALYSIS

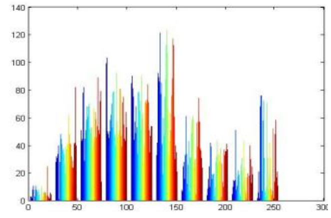
	MSE	RMSE	PSNR
Xylophone.mpeg	2.6996e+003	51.9579	13.8178
Shaky_car.avi	2.3159e+003	48.1235	14.4837
Vipmosaicking.avi	3.5655e+003	59.7120	12.6096
Rhinos.avi	3.1967e+003	56.5391	13.0838
Vipsnowydays.avi	3.2019e+003	56.5851	13.0768

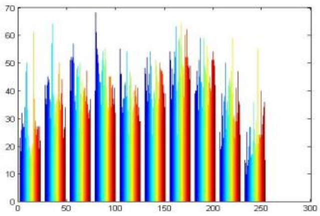
Table 1 Performance of our encryption scheme

4.3 HISTOGRAM FOR FRAME

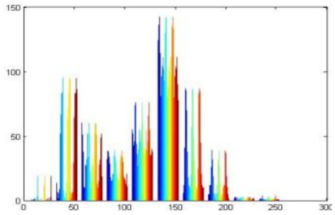
Before Encryption After Encryption

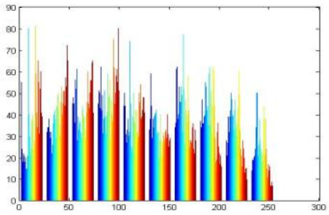
1. Xylophone Video



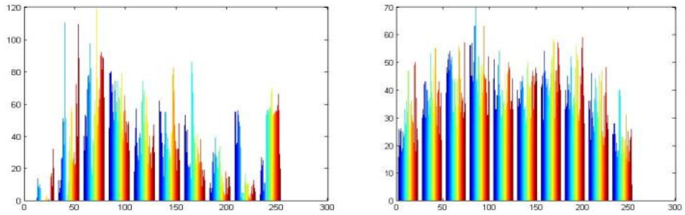


2. Shaky_car

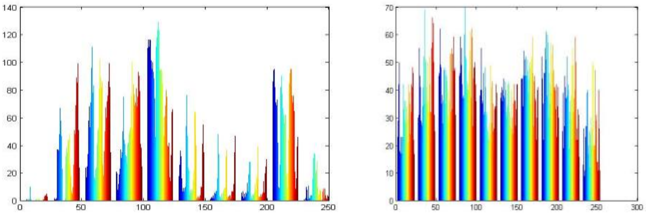




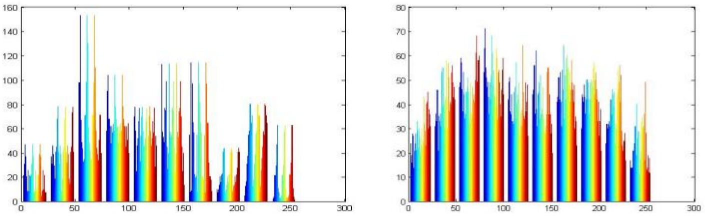
3. Vipmosaicking



4. Rhinos



5. Vipsnowydays



5. CONCLUSION

We also present an extended classification of digital video encryption algorithms in order to clarify these advantages. We analyze both security and performance aspects of the proposed method, and show that the method is efficient and secure from a cryptographic point of view. Experiments were conducted to demonstrate that video-Frame encryption provides a good trade-off between encryption robustness, flexibility, and real-time processing

Even though the method is currently feasible only for a certain class of video sequences and video codes, the method is promising and future investigations might reveal its broader applicability. Finally, we extend our approach into a novel type of digital video steganography where it is possible to disguise a given video with another video. For future research, it is proposed that this novel scheme be developed to full encrypt video sequences. The following are some point to improve our proposed system. Further improvement to the security level can be achieved by encrypting the I-Frame blocks in P- and B-Frames. This will increase the security level, considerably Enhance the proposed system security by encrypting the motion vector of the frames. Further we will extend this work on secret image sharing Scheme which provide a more security.

6. REFERENCES

[1] Tuchman W.: A brief history of the data encryption standard. ACM Press Addison-Wesley Publishing Co., New York (1997))

[2] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., et al.: A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering 1 (1), 70…75(2007).

[3] Cormen, T. H., Leiserson, C. E., Rivest, R. L., Stein, C.: Introduction to algorithms, 2ndedn. MITPress, McGraw-Hill,Cambridge(2001)

[4] Y. Zhou, S. Agaian, V. M. Joyner, and K. Panetta, "Two Fibonacci P- code based image scrambling algorithms," in Image Processing: Algorithms and Systems VI, San Jose, CA, USA, 2008, pp. 681215-12.

[5] D. Socek, H.Kalva, O. Marques, D. Culibrk, B.Furht : “New Approaches to encryption and steganography for digital videos”, Multimedia Systems DOI10.1007/s00530-007-0083-z,Springer-Verlag 2007.

[6] Devaney, R. L. :An introduction to chaotic dynamical systems, 2nd edn.West- view Press, San Francisco (2003).

[7] Alligood, K. T., Sauer, T., Yorke, J. A. : Chaos: an introduction to dynamical systems. Springer, Heidelberg (1997).

[8] Yang, T., Wu, C. W., Chua, L.O. : Cryptography based on chaotic systems. IEEE Transactionson Circuits and Systems-I : Fundamental Theory and Applications 44, 469…472 (1997).

[9] Solak, E. : Cryptanalysis of observer based discrete-time chaotic encryption schemes. International Journal of Bifurcation and Chaos 15 (2), 653…658 (2005).

[10] He, J., Qian, H., Zhou, Y., Li, Z.: Cryptanalysis and improvement of a block cipher based on multiple chaotic systems. Mathematical Problems in Engineering 2010,1…14 (2010).

[11] Yicong Zhou, Karen Panetta, Sos Agaian “Image Encryption Using Binary Key-images” Proceedings of the 2009 IEEE International Conference on Systems Man and Cybernetics San Antonio TX, USA-October 2009.

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

[13] 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.

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

[15] Agi, I., & Gong, L. (1996). An emprical study of MPEG video transmissions. Proceedings of The Internet Society Symposium on Network and Distributed System Security (SNDSS 96) , 137.144.

[16] Salah, A. (2003). A Light-Weight Encrypting For Real Time Video Transmission. Retrieved Nov 2008, 22, from http://www.cdm.depaul.edu/legacy/checksite.aspx?oldUrl=http://www.cdm.depaul.edu/research/Documents/TechnicalReports/2004/TR04-002.pdf

[17] Habib Mir M., H., & Pong Mee, T. (2006). Encryption of MPEG Video Streams. 2006 IEEE Region 10 Conference TENCON 2006. 1-4. Hong Kong, China.

[18] Tang, L. (1996). For encrypting and decrypting MPEG video data e±ciently. in Proceedings of The Fourth ACM International Multimedia Conference (ACM Multimedia'96), (Bosten, MA). 219-230.

[19] Gulistan, R., & Muhammad, J. M. (2004). Performance Comparison of Advanced Video Coding H.264 Standard with Baseline H.263 and H.263+ Standards. IEEE International Symposium on Communications and Information Technology, 2004. ISCIT 2004. 743-746

[20] Ashrux, G., & Chong, M. N. (1997). Performance analysis of H.261 and H.263 video coding algorithms . Proceedings of IEEE International Symposium on Consumer Electronics (ISCE '97), 153-156.

[21] Karel, R. (1996). H.263: video coding for low-Bit-Rate Communication. IEEE Communications Magazine, Volume: 34, Issue: 12. 42 - 45.

[22] Sikora, T. (1997). MPEG digital video-coding standards. MPEG digital video-coding standards , Pp 82 - 100.

[23] Morris, O. (1995). MPEG-2: where did it come from and what is it? IEE Colloquium on MPEG- 2 - What it is and What it isn't. 1-5 . 143

[24] Adolfo, R., David, K. F., & Steven, C. B. (1996 Jule). MPEG-2 Fundamentals for Broadcast and Post-Production Engineers. A Video and Networking Division White Paper, 1-21.

[25] Atul, P., & Alexandros, E. (1998). MPEG-4: An object-based multimedia coding standard supporting mobile applications. Mobile Networks and Applications 3, 5-32.

[26] MPEG-4. (2002). Overview of the MPEG-4 Standard. Retrieved JAN 02, 2009, from http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm.

[27] Cheng, H., & Li. (2000). Partial encryption of compressed images and videos. IEEE Transactions on signal processing, 2439-2451

[28] Olivier, A., & Philippe, S. (2001). MPEG-7 Systems: overview. IEEE Transactions on Circuits and Systems for Video Technology. 760-764.

[29] Martínez, J. M. (2002). Standards - MPEG-7 overview of MPEG-7 description tools, part 2. IEEE Multimedia,Volume : 9, Issue:3. 83 - 93 .

[30] Atul, P., Xuemin Chen, & Ajay Luthra (2004). „Video coding using the H.264/MPEG-4 AVC compression standard. Signal Processing: Image Communication 19, 793–849.

[31] Othman, 0. K., Islam, M., Khan, S., & Shebani, M. (2004). Communications Cryptography. RF and Microwave Conference, (RFM 2004). Proceedings. 220-223.

[32] Kessler, G. C. (1998). An Overview of Cryptography. Retrieved 20 Des, 2008, from http://www.garykessler.net/library/crypto.html#intro.

[33] David, K. (1980). Cryptology goes public. IEEE Communications Magazine, 19- 28.

[34] White, B. (2003). Cisco Security+ Certification: Exam Guide. McGraw-Hill.

[35] Harris, S. (2007). CISSP® All-in-One Exam Guide. McGraw-Hill.

[36] Federal Information processing standand. (1999). Data Encryption Standard (DES). Retrieved Des 20, 2008, from http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[37] Whitfield, D., & Hellman, E. M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory. 644--654.

[38] Agi and L. Gong. An empirical study of MPEG video transmission. In Proc. of the Internet Society Symposium on Network and Distributed Systems Security, pages 137–144,1996.

[39] T. B. Maples and G. A. Spanos. Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video. In Proc. of Fourth International Workshop on Multimedia Software Development ’96), 1995.

[40] L. Qiao and K. Nahrstedt. A new algorithm for MPEG video encryption. In Proc. of First International Conference on Imaging Science System and Technology, pages 21–29,1997