RESEARCH ARTICLE OPEN ACCESS

Video Encryption Algorithm and Key Management using Perfect Shuffle

Sayyada Fahmeeda Sultana *, Dr. Shubhangi D C**
**(Department of Computer Science, PDA College Engineering, Kalaburagi, Karnataka*
sayyadafahmeeda@gmail.com)
*** (Department of Computer Science, VTU PG Center, Kalaburagi, Karnataka*
shubhangidc@vtu.ac.in)

ABSTRACT
Advancements in networking technologies like cloud computing have popularized applications like, Video-On Demand (VOD), video conferencing, pay-per-view, video broadcast, etc, in all such applications, confidentiality of the video data during transmission in network and during storage is extremely important. This necessitates secure video encryption algorithms suitable for multimedia application because of the large data size and real time constraint. Conventional encryption algorithms are designed for generic data, and as such, it does not support many specific video application requirements. In the paper we propose a computationally efficient and secure video encryption algorithm that makes encryption feasible for real-time applications without heavy computational overhead and reduces key management by utilizing block shuffling technique. Block Shuffling based video encryption with Faro IN OUT Shuffle and rotation, i.e., first image is rotated by an angle then key is generated based Block size using Faro IN OUT perfect shuffle which is a perfect shuffling algorithm which is isomorphic to random permutation. we will show that our proposed method provide more scrambling of image then random permutation and no need to maintain long key file.

Keywords: Block Shuffling, Faro Perfect Shuffle, Key Management, Mean Squared Error, Peak Signal to Noise Ratio, Pure Random Permutation, Structural Similarity Index Measure, Video Encryption

I. INTRODUCTION

Security is becoming escalating concern in increasing multimedia defined world. With continuing development of network communications, fast advances in Internet technology, easily capturing of videos and cloud computing systems multimedia data are of importance for use more and more widely, in applications such as video-on-demand, video conferencing, broadcasting, etc. as it is closely related to many aspects of daily life, including education, commerce, entertainment, defense and politics. In order to maintain privacy or security sensitive data need to be protected before transmission or storage.

Authorized user only can get back the original content using the decryption algorithm. Encrypting, a block cipher might take an n-bit block of plaintext as input and output a corresponding n-bit block of cipher-text. Exact transformation is controlled using a second input – the secret key. Decryption is similar, takes an n-bit block of cipher-text together with the secret key and outputs the original n-bit block of plaintext. Block-ciphers examples are RC5, AES, DES, Blowfish, many more. In this case we use block shuffling in each frame to perform encryption decryption is performed by re-shuffling blocks back.

Categorization of Video Encryption Algorithms

- Layered Encryption, in this technique videos frames are encrypted using DES, IDEA, AES, RSA, etc. those techniques are not suitable for real time applications due to speed limitations
- Selective Encryption, encrypt the bytes in frame that require more security to reduce computational complexities
- Permutation based Encryption, use scrambling of frame to encrypt, random numbers are used as key to scrambling process.
  The work is motivated to provide video security through block shuffling with key generated using Faro IN OUT shuffle rather than random permutation.

Random Permutation

Random permutation a random ordering of a set of objects, i.e, a permutation valued random variable. The use of random permutations is often fundamental to fields that use randomized algorithms such as coding theory, cryptography, and simulation.
Generation of a random permutation for a set of length n uniformly at random interval is generated as sequence by taking a random number between 1 and n sequentially, ensuring no repetition, and

interpreting this sequence (r1, ..., rn) as the permutation shown below equ. (1).

$$\begin{pmatrix} 1,2,3,\dots,n \\ r1,r2,r3,\dots,rn \end{pmatrix} \quad (1)$$

Image Shuffler: Key Generation using Faro Perfect Shuffle

Perfect shuffle is a permutation of n elements each shuffle produces a new permutation or returns to a previous at some point the process would return to the original order. Moreover, there are n! set of n elements. The key generated group generated using Faro perfect shuffle is a non-random process.

There are two ways to perfectly shuffle using faro in and out shuffle. The process Key generation starts by deciding the number of blocks in an image (natural number - 2n blocks), both the methods cut the number 2n into half's and interlace perfectly. The in shuffle 'I' leaves the original first block at second block position. The out shuffle '0' leaves the original first block on correct position. Let the blocks be labeled $(0,1,\dots,n-1,n,\dots,2n-1)$. After an in shuffle the order is $(n,0,n+1,\dots,2n-1,n-1)$. After an out shuffle, the order is $(0,n,l,n+l,\dots,n-1,2n-1)$.

The proposed algorithm use a combination of In and Out faro shuffles to generate a group, this group will be called the shuffle group and denoted (I, 0). Both of the methods preserve symmetry at the center (0 and 2n - 1, 1 and 2n - 2, etc.) are sent to symmetric positions about the center. Thus (I, 0) is a subgroup of the centrally symmetric permutations. This group is isomorphic to the Weyl group (The Weyl group is isomorphic to the group of permutations [11]) B_n. Where Bn is the hyper-octahedral group Bn is the group of all permutations w of $(kl,\dots,kn)$such that$\sim(4) = -w(i)$for i $= 1.2\dots,n$. The order of Bn is n! 2n

Further, paper is organized as follows: Section II, gives the proposed video encryption algorithm. Experimental analysis of results showing the performance of proposed algorithms compared with other state of art method given in Section III. Lastly, Section IV serves to present our conclusions and ideas for future work related to this research.

II. PROPOSED VIDEO ENCRYPTION ALGORITHM

The Proposed algorithm for video encryption works on individual frames. Each frame goes through Algorithm 1, Algorithm 2, all the frames are combined to form an encrypted video.

Algorithm 1: *Key Generation Using Faro Perfect Shuffle*

Input: *Frame Size MXN, Block Size B*
Output: *An Array of Integers K*
Step 1: *Find number of Block in frame '2n' using frame size and block size*
Step 2: *Divide n into two halves* $(0,1,\dots,n-1,n,\dots,2n-1)$
Step 3: *Interlace the divided halves using In Shuffle I* $(n,0,n+1,\dots,2n-1,n-1)$
Step 4: *Apply out shuffle on O Out shuffle* (I)
Step 5: *return Key* $K \leftarrow O,B$

Algorithm 2: *Frame Encryption using Block Shuffling*

Input : *Frame* F_i *where* $i = 1,2\dots,n$, *Block Size B, Number of Blocks* $2n$
Output : *Perfectly Shuffled Frame* F_i'
For each $i = 1,2,\dots,n$
Step 1: $R_i \rightarrow$ *Rotate* F_i $(90°\ or\ 180°)$
Step 2: *Use Algorithm* 1 *for key generation*
Step 3: *Use Block Size B to logically divide* R_i *into* $2n$ *blocks*
Step 4: $F_i' \leftarrow$ *Perform Block Shuffling based on blocks generated in step*3 *using Key K*

Decryption is analogies with encryptions provided the receiver of frames has the same degree of rotation, block size, order of faro shuffle.

III. EXPERIMENTAL RESULTS

In order to evaluate the performance of the proposed encryption scheme, The video data used for analysis have different motion characteristics and varying resolution with a frames rate of 25 fps. The sample test video sequence include videos toy_plane, bar_100, table_tennis, pond, etc. A good encryption procedure should be robust against all kind of cryptanalytic, statistical, differential and brute-force attacks. Thus the histogram of the ciphered frame must not be uniform with original frame to avoid statistical attacks, and the key space must be large enough to avoid brute force attacks. Below show the performance analysis of the proposed approach.

3.1 Histogram Analysis of Frames

In proposed experiment the plain frame and its corresponding ciphered frame histograms are shown in Fig. 1.

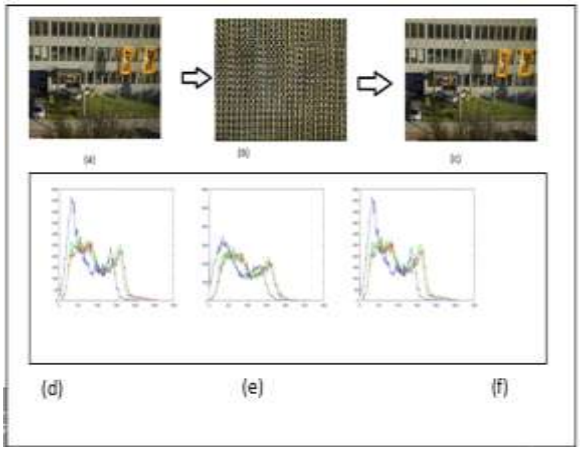

Fig.1. (a) Original Frame, (b) Encrypted Frame, (c) Decrypted Frame, (d) Color wise histogram of figure 1(a), (e) Color wise histogram of figure 1(b), (f) Color wise histogram of figure 1(c)

3.2 Numerical Analysis

For qualifying the visual distortion, the visual results are illustrated in figure(1), we provide in this section a numerical analysis of the proposed Block Shuffling algorithm with rotation and In out Faro perfect shuffle to describe the scrambling effect on video frames in comparison with other state of art method of Random permutation on images. The metric used in [8] to describe the scrambling effect on video contents are peak signal-to-noise ratio (PSNR), the Structural Similarity measure index(SSIM) and MSE Mean Squared Error. These computations allows us to efficiently describe the losses in quality (PSNR) measured in dB and in structural coherence (SSIM)

3.2.1 Peak Signal to Noise Ratio (PSNR)

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale shown in equ(2).

$$PSNR = 10log_{10}\left(\frac{(Max\ possible\ pixel\ value\ of\ Image)^2}{Mean\ Squared\ Error}\right) \quad (2)$$

In Fig. 2, we use PSNR to compare the scrambling effect of our proposed method of "Block Shuffling with rotation and key generated using IN out group" with frames scrambled using random permutation.

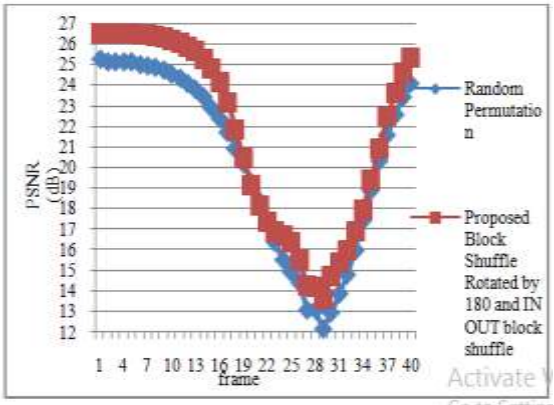

Fig.2. Frame-by-frame numerical analysis of PSNR of proposed method with Random Permutation

The larger value of PSNR indicated more distorted frame. The proposed method provides higher PSNR compare to Pure Random Permutation.

3.2.2 SSIM and MSE Measure

Structural Similarity Index of Ciphered frame with Original Frame the Structural Similarity (SSIM) index is a method for measuring the similarity between two images gives the formula for SSIM as in equ (3).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

Where $\mu_x \rightarrow$ *the avearge of* $x, \mu_y \rightarrow$ *the avearge* y,

σ_x, σ_y *and* σ_{xy} *are variance of* x, *variance of* y *and covariance of* x, y, *respectively*.

$c_1 = (K_1\ L)^2, c_2 = (K_2\ L)^2$: two variables to stabilize the division with weak denominator; L the dynamic range of the pixel-values (typically this is $2^{No.of\ bits/pixel} - 1$);$K_1 = 0.01$ and $K_2 = 0.03$ by default.

3.2.3 Mean Squared Error (MSE) :

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(F_i' - F_i)^2 \quad (4)$$

where n is the number of pixels in a frame $\boldsymbol{F_i'}$, the encrypted frame, and $\boldsymbol{F_i}$ the original frame

Fig. 3. Shows the comparison of SSIM and MSE for proposed method with Pure Random Permutation

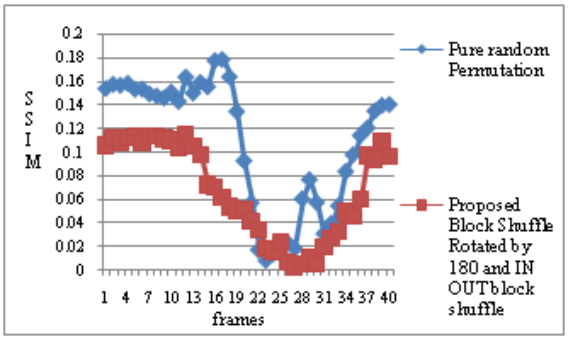

Fig. 3. SSIM for Proposed method with Pure Random Permutation

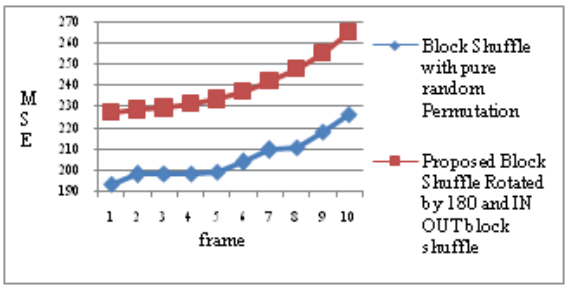

Fig. 4. MSE for Proposed method with Pure Random Permutation

Proposed method provides SSIM closer to zero then Pure Random Permutation, and Higher MSE by this we can say that the proposed method provides more scrambling of image then Random-permutation.

3.2.4 Other Consequences of Encryption with other state of art methods

Time:

Time taken to encrypt a frame of size 128x128 pixels with different block sizes is shown in Table 1. A Comparison of encryption time of our proposed method with other state of art methods is given in Fig. 5. It can be observed that the smaller the block size more secure will be the image so using 2 pixels per block encryption time per frame of size 256 pixels the proposed encryption algorithm took 0.252779 seconds, which is less than that of other techniques Blowfish, Rijndael, DES [6] for an image with 256 pixels. This makes our algorithm more suitable for real-time video encryption.

Table 1. Time to Encrypt frame with different block sizes

Block Size (pixels per block)	Frame (128 X 128) pixels Encryption Time in seconds
64	0.002628
32	0.003354
16	0.039413
8	0.016458
4	0.061489
2	0.285943
1	1.114790

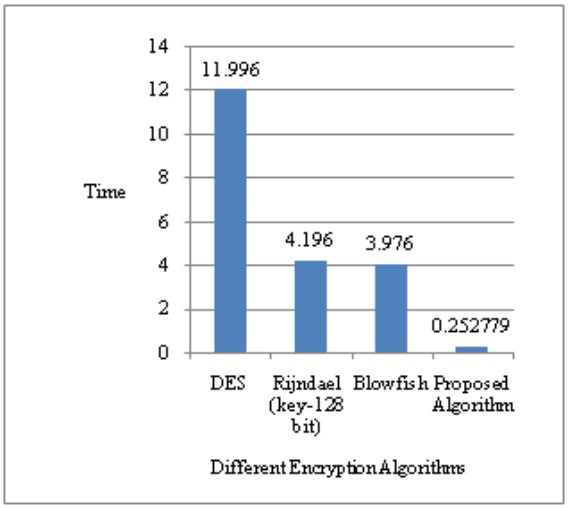

Fig. 5. Encryption time of different encryption algorithms

Key Management:

The proposed method uses the key as block size, key generation pattern, angle of rotation of image which takes far smaller amount of memory then Pure Random Permutation method which requires a text file to be maintain for each video to store key. The file size will increase as the number of blocks increases. But our proposed method provide high level of security without the need to maintain text file. The proposed method is more suitable for real-time application.

IV. CONCLUSION AND FUTURE WORK

In this paper, in contrast to the conventional system of Pure Random permutation, we proposed a Block Shuffling based video encryption with Faro IN OUT Shuffle and rotation, i.e., first image is rotated by an angle then key is generated based Block size using Faro IN OUT perfect shuffle which is a perfect shuffling algorithm which is isomorphic to random permutation. Further we showed that our proposed method provide more scrambling of image then random permutation. Future enhancement to the proposed approach can be done by compressing the video.

REFERENCES

[1] Jian Zhang, Xuling Jin, "Encryption System Design Based on DES and SHA-1",11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science, IEEE 2012.

[2] Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo, "Recent Advances in Multimedia Information System Security", International Journal of Computing and Informatics, Vol. 33, No.1, 2009, pp. 3-24.

[3] Shiguolian,"Multimedia Content Encryption Algorithms and Application", CRC Press 2008.

[4] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar, "Fast and Secure Real-Time Video Encryption", Sixth Indian Conference on Computer Vision, Graphics & Image Processing, IEEE, 2008, PP.No. 257-264

[5] Mrinal Paliwal, Saddam Hussain, "Selective Video Encryption using Bit XOR Technique", International Journal for Innovative Research in Science & Technology-Volume 2, Issue 1, June 2015, PP. No. 177-183

[6] Simon Fong, Yang Hang, "On Improving The LightWeight Video Encryption algorithms for Real Time Video Transmission", 3rd International Conference on Communications and Networking In China, IEEE 2008.

[7] B.Furht, D. Socek, and A M Eskicioglu, "Fundamentals of Multimedia Encryption Techniques", Multimedia Security Hand book, CRC Press 2005.

[8] Abdel-karim, Al Tamimi, "Performance analysis of Data Encryption Algorithm", http://www.cse.wustl.edu/jain/cse567-06/ftp/encryption_perf/index.html, PP No. 1-13

[9] Jolly shah, Dr. Vikas Saxena, "Video Encryption: A Survey", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011, PP.No. 525-534

[10] Cao Guang-hui, Hu Kai , Yang He and E Xu, "Algorithm of Image Encryption based on Permutation Information Entropy", 3rd International Conference on Computer and Electrical Engineering, 2010

[11] Persi diaconis, "The Mathematics of Perfect Shuffles",Advances In Applied Mathematics 4, 175-196 (1983), PP. No. 175-196

[12] RamandeepKaur, Pooja, "A hybrid approach for video steganography using edge detection and identical match techniques", International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE March 2016

International Journal of Engineering Research and Applications (IJERA) is UGC approved Journal with Sl. No. 4525, Journal no. 47088.

Sayyada Fahmeeda Sultana. " Video Encryption Algorithm and Key Management using Perfect Shuffle." **International Journal of Engineering Research and Applications (IJERA)** 7.7 (2017): 01-05