International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-8, June 2020

BITS – A Novel Video Encryption Algorithm

K.Subraja, N.Geetha, K.Mahesh

Abstract**: *Increased digital information exchange poses a major threat against confidentiality of the information being shared. The information exchange among the parties is said to be efficient only if the transmission process is secure and withstand security breaches. The information shared may be text, image, audio or video. Because of the availability of Internet facility around the world, video became the prime source of information exchange. We all know that anything in the form of visuals will reach the target audience in an efficient manner. They are considered as the major component of the education sector. This paper proposes a novel real time video encryption called BITS. BITS is nothing but Blocking-Inverse-Transposition-Substitution. Initially the video frames are divided into four blocks and the block contents are inverted. Then the entire content of the frame is transpositioned based on the key. And finally the contents of the frame is substituted with different random value. This proposed algorithm is strong against brute-force and statistical attack. The proposed algorithm is suitable for all real time multimedia environments. This algorithm is a compression independent one. The first two phases of the BITS algorithm are implemented using MatLab. The time taken for the computation steps are recorded and analyzed in this paper.***

Keywords : Information Security, Video encryption, BITS, Confidentiality

I. INTRODUCTION

Recent advancements in the Information and Communication Technology have made video communications simpler. Users across the world are making use of applications [3] such as virtual learning through video broadcast, on demand video streaming, video conferencing etc. Videos are a more powerful and communicative media that can capture and present information. In recent times large video databases are created because of the advancements in many video acquiring devices and internet [7].While experiencing the ease in video information sharing, confidentiality of the data is under threat. MPEG [1] is the most commonly used simple video encryption approach. This approach treats the entire information as text data and employs standard encryption algorithms over it. To overcome the computational complexity in this approach selective encryptions [1, 2, 5] are proposed. These algorithms are well known as light weight real time encryption algorithms. The computational overhead is reduced through these algorithms. When compared to the traditional cryptography, the authors of [3] addressed the importance of chaos-based cryptography. The chaos-based cryptography algorithms are easy to implement and suitable for large scale video encryption. The Puzzle [4] video encryption algorithm is best suitable for encryption of video streams. It is a compression independent encryption algorithm. The efficiency of the video encryption algorithms are justified in terms of computational overhead and time complexity.

The research work is documented as given below. The existing works are elaborated in section II. The proposed BITS algorithm and its phases are described in section III. The results of the first two phases of the proposed work and its time complexity are discussed in section IV. The conclusion and future work of the research work is presented in section V.

II. REVIEW OF LITERATURE

Video Processing is rapidly growing technologies. It is a strategy to play out a few tasks on a video, to get an upgraded video or to separate some helpful data from it [12].This research work is motivated by the following existing works. Hamidouche et al [3] proposed a selective video encryption for HEVC standard. The authors used chaos-based generator and is implemented using Scalable Reference Software Model encoder. The authors analyzed the performance of the proposed methods using metrics like histogram analysis, encryption time and video quality. Raju et al [6] proposed a fast and secure real time video encryption algorithm. RC5 algorithm is used for encrypting the DCT coefficients in this work. This algorithm is compression based one and slightly decreases the compression rate which is compromised for high security. The average encryption time per frame of the algorithm proposed is around 8.32ms. The authors of [8] proposed a color image cryptosystem via hyper chaos synchronization. This work combines the technology of both traditional cryptography and spatial domain encryption. The encryption consists of image pixel value substitution with diffusion matrices and permutation with scrambling matrices. The results of the proposed algorithm are analyzed using histogram analysis, correlation analysis of adjacent pixels, noise and crop attacks analysis. K-N secret sharing scheme is proposed in [9], where the image is encrypted by dividing the image into N number of shares and the image can be retrieved with the help of stacking at least K shares. The image related encryption and decryption process were clearly discussed in this work and the performance is analyzed using PSNR and 4PSNR.

Revised Manuscript Received on June 30, 2020.

***** Correspondence Author

K.Subraja*,M.Phil Student, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India. Email: subrajakamaraj.k@gmail.com

N.Geetha, Ph.D Scholar, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India. Email:geetha.researchscholar@gmail.com

Dr.K.Mahesh, Professor, Department of Computer Applications, Alagappa University, Karaikudi, Tamilnadu, India. Email:mahesh.alagappa@gmail.com

Zeng et al [10] proposed a novel approach for efficient video encryption. This approach combined the features of both encryption and compression techniques. The video is scrambled in the frequency domain. Operations such as shuffling, rotation, selective bit sampling are employed. The proposed methodology of the authors withstand security attacks and offers different levels of transparency. Wen et al [11] described the application for securing MPEG-4 video content in wireless environment. The properties of the protected as well as the unprotected bit streams are studies to incorporate error control. The outcome of the work is standard compatible compressed video. It will be best suitable for wireless transmission.

The following section will describe the proposed BITS video encryption algorithm.

III. BITS VIDEO ENCRYPTION ALGORITHM

The proposed BITS (Blocking – Inverse – Transposition – Substitution) video encryption algorithm consists of six phases. The phases and their work are explained in this section. The architecture of the BITS encryption process is given below.

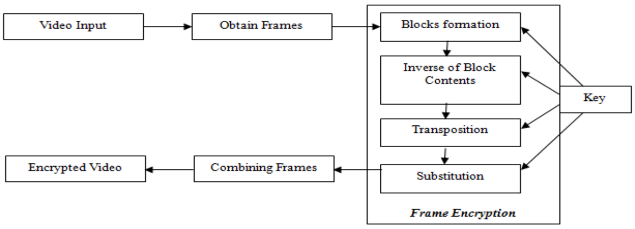


Fig. 1.Architecture diagram for BITS Encryption process

A. Framing

All the video contents consist of frames. Many of the video encryption algorithms perform the encryption at the frame level. The proposed BITS algorithm follows the same principle. The first phase of the proposed methodology is to divide the video into frames. The frames are given as inputs to the frame encryption process which in turn consists of four sub processes. The process of the BITS encryption is explained with the help of the example frame with size 4x4. The following figure illustrates one such frame generated through the framing process.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Fig. 2.Sample Frame

B. Key generation

Every encryption algorithm is working based on a key. This algorithm is a symmetric encryption algorithm. The random key is generated in this phase. The size of the key is based on the size of the frame. The selective portions of the key are used for the following four sub processes of frame encryption. With reference to the sample frame shown in figure 2, the key is generated with the same size i.e. 4x4. The key is shown in the following figure. From the key generated, four keys are generated namely K1, K2, K3 and K4. Based on the keys generated the following phases will be processed to create the encrypted frame.

K1	0	1	0	0	4
K2	0	0	1	1	3
K3	0	0	1	0	2
K4	0	0	0	1	1

Fig. 3. Sample key generation

C. Blocks formation

The frames thus obtained from the first phase are considered as inputs. The frames are further divided into blocks. The number of blocks is determined by the key value. The randomly generated key portion is used to identify the number of blocks and size of the blocks. In the above figure 3, based on the key value K1, the image is divided into four blocks. The formation of the block is represented in figure 4.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Fig. 4. Image divided into 4 blocks

D. Inverse of Block contents

Once the blocks are formed for the frame, the content of the block is used for this phase. The block is considered as a matrix and inverse of the matrix is found. This will shuffle the contents within the block. The portion of the key value is used while finding inverse of the block contents. The divided frames are then inversed to form the inverted block contents. Here the rows are changed into columns and the columns are changed into rows. The conversion is done within every block.

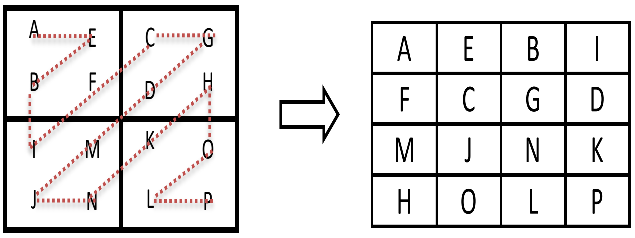
A	E	C	G
B	F	D	H
I	M	K	O
J	N	L	P

Fig. 5.Inversed block content

E. Transposition

The entire frame is considered in this phase. The frame contents are trans-positioned based on the portion of the randomly generated key value. This will further confuse the contents of the frame. The contents will be rearranged and isgiven as input for the next phase. For the transposition process, the four keys are used.

The order is K4, K3, K2 and K1. Transposition is applied on the frame contents entirely irrespective of the blocks. The transposition result is shown below.



A	E	B	I
F	C	G	D
M	J	N	K
H	O	L	P

Fig. 6. Transposition of the frame contents

The transposition of the frame is performed by considering the number of pixels one, two, three and four (values of K4, K3, K2 and K1) at a time. The transposition process is depicted below.

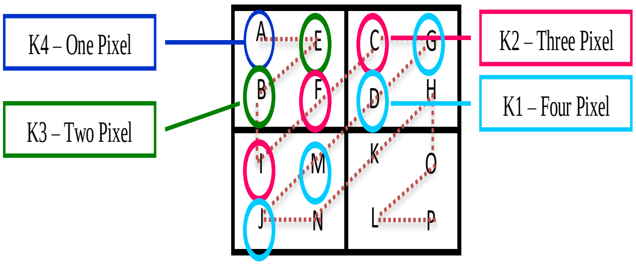


Fig. 7. Transposition process based on the key generated

Once the transposition process incorporated the entire key file, the reverse order is performed. The transposition order would be K4, K3, K2, K1, K2, K3, and finally K4. This process will be repeated until all the pixels are covered in the frame.

F. Substitution

Simply rearranging the contents alone will provide some hits to the advisories. In order to overcome that, the last phase of the proposed algorithm will perform substitution based on the portion of the random key. The substitution is designed in such a way that the same contents of the frame will be substituted with different values. This will overcome the statistical attacks. Here the substitution is done with the help of the key K4. Each pixel value is substituted by its next immediate pixel values.

B	F	C	J
G	D	H	E
N	K	O	L
I	P	M	Q

Fig. 8. Frame contents after substitution phase

The encrypted frames are then combined to form the encrypted video. Even though same key is used in all the phases of the BITS algorithm, the portion of key used for the each phase varies. This will definitely reduce the risk of guessing the key values used by each phase. The same process is reversed to generate the decrypted video.

IV. RESULTS AND DISCUSSION

The BITS algorithm is implemented using MatLab software. Following figure is a sample frame generated while implementing the proposed method. The FlickAnimation.avi video file with 1.52 KB size is given as sample input to the proposed work. The results of the video encryption are discussed below. The first frame of the video is shown in the following figure.

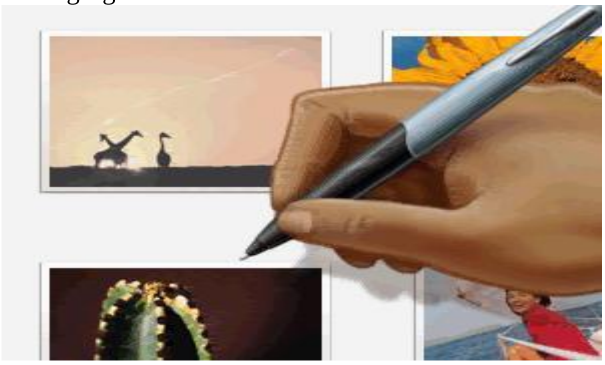
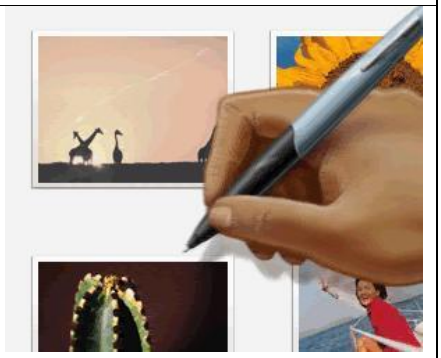
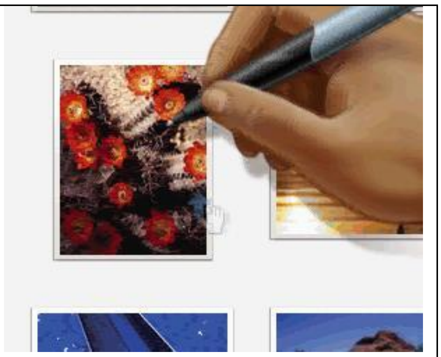
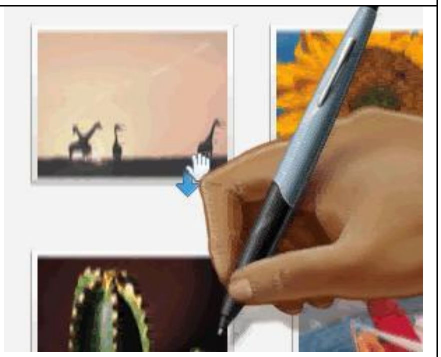
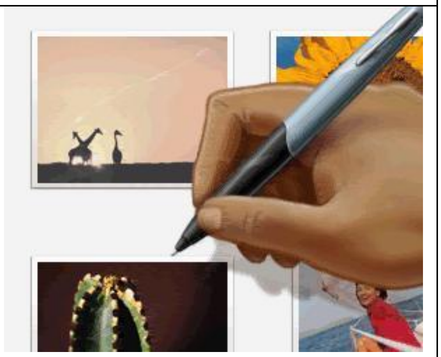


Fig. 9. First frame of FlickAnimation.avi

Totally this file consists of 59 frames. Some other frames of the sample video are tabulated below. The generated frames will be processed individually to find the encrypted frame. Once all the frames are encrypted, it can then be converted back to video file.

Table I. Sample frames of FlickAnimation.avi

Frame Number	Frame
3	
18	

30	
50	
59	

The encrypted frame is shown below. From the encrypted frame it is clear that the encryption is done in an efficient manner. The proposed method will withstand the brute force attack also.

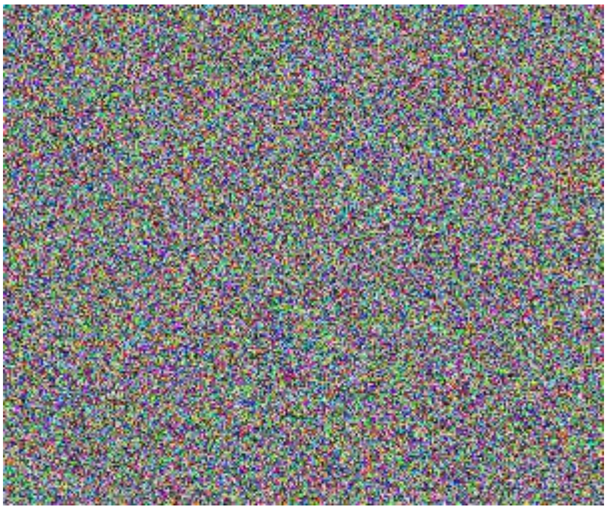


Fig. 10. Encrypted frame of figure 9

The execution time for a sample video to perform the BITS algorithm is 9.53 milli seconds. Similarly the implementation is tested with some other videos with the maximum frame count restricted to 129. The average execution time is around 9-12.5 milli seconds. The work is to be implemented with other benchmarks videos also.

V. Conclusion

This research work proposes a novel BITS (Blocking – Inverse – Transposition – Substitution) algorithm for video encryption. The proposed algorithm is compression independent algorithm. The strength of the proposed algorithm lies in its key. The size of the key varies with respect to the size of the frames generated. The randomness property of the key assures secure data transmission across the network. The same portion of the key is not used by all the phases of the frame encryption. Different portions are used by different phases. This will prevent the brute force attack. The phases are implemented using MatLab and the execution time is measured. The further work will implement the remaining three phases of the proposed BITS algorithm. The video encryption quality metrics are to be analyzed in the future work. This novel algorithm will be implemented easily in all environments and will provide better security to the user. By implementing this algorithm the videos can be efficiently transmitted thereby assuring the confidentiality of the video content.

REFERENCES

1. I. Agi and L. Gong, "An empirical study of secure MPEG video transmissions," Proceedings of Internet Society Symposium on Network and Distributed Systems Security, San Diego, CA, USA, 1996, pp. 137-144.
2. G. A. Spanos and T. B. Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video," Proceedings of Fourth International Conference on Computer Communications and Networks - IC3N'95, Las Vegas, NV, USA, 1995, pp. 2-10.
3. Hamidouche, Wassim & Farajallah, Mousa & Sidaty, Naty & El Assad, Safwan & Déforges, Olivier. (2017). Real-Time Selective Video Encryption based on the Chaos System in Scalable HEVC Extension. Signal Processing: Image Communication. 58. 10.1016/j.image.2017.06.007.
4. Liu F., Koenig H. (2005) Puzzle – A Novel Video Encryption Algorithm. In: Dittmann J., Katzenbeisser S., Uhl A. (eds) Communications and Multimedia Security. CMS 2005. Lecture Notes in Computer Science, vol 3677. Springer, Berlin, Heidelberg
5. Choo, E., Lee, J., Lee, H., & Nam, G. (2007). SRMT: A lightweight encryption scheme for secure real-time multimedia transmission. In Proceedings - 2007 International Conference on Multimedia and Ubiquitous Engineering, MUE 2007 (pp. 60-65). [4197250] https://doi.org/10.1109/MUE.2007.194
6. C. N. Raju, G. Umadevi, K. Srinathan and C. V. Jawahar, "Fast and Secure Real-Time Video Encryption," 2008 Sixth Indian Conference on Computer Vision, Graphics & Image Processing, Bhubaneswar, 2008, pp. 257-264.
7. Gayathri, N., & Mahesh, D. K. (2018). A Systematic Study on Video Indexing. International Journal of Pure and Applied Mathematics, 118(7), 207-213.
8. Wu, Xiangjun & Bai, Chenxi & Kan, Haibin. (2014). A new color image cryptosystem via hyperchaos synchronization. Communications in Nonlinear Science and Numerical Simulation. 19. 1884–1897. 10.1016/j.cnsns.2013.10.025.
9. Vignesh. M1, Raihana. P.A2, Shahadha Hakkim3, Sukanya. S (2018), An Efficient K-N Secret Sharing Image and AES Encryption Algorithm in Visual Cryptography, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 2, February 2018, pp. 233-239.
10. Zeng, W., & Lei, S. (2003). Efficient frequency domain selective scrambling of digital video. IEEE Transactions on Multimedia, 5(1), 118-129.

11. Jiangtao Wen, M. Severa, Wenjun Zeng, M. H. Luttrell and Weiyin Jin, "A format-compliant configurable encryption framework for access control of video," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 12, no. 6, pp. 545-557, June 2002.
12. Gayathri, N., & Mahesh, K. (2018, December). A Generic Approach for Video Indexing. In International conference on Computer Networks, Big data and IoT (pp. 701-708). Springer, Cham.

AUTHORS PROFILE

K.Subraja is a M.Phil candidate in the Department of Computer Applications, Alagappa University, Karaikudi. Tamilnadu, India. Her area of interest includes Video Security.

N.Geetha is a Ph.D Scholar in the Department of Computer Applications, Alagappa University, Karaikudi. Tamilnadu, India. Her area of interest includes Video Processing (Encryption) and Cloud Security.

K.Mahesh is a Professor in Department of Computer Applications, Alagappa University, Karaikudi, India. He has Published many papers in Peer-Reviewed and Reputed Journal and has 25 years of experience in teaching. His research interests are Video Segmentation, Video Processing and Image Processing.