Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2463

Enabling Secured Data Transfer with Encryption based on Binary Conversion

Akash Chauhan
Asst. Professor, Department of Comp. Sc. & Info. Tech.,
Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number:1725 - 1733
Publication Issue:
Vol 70 No. 2 (2021)

Article History
Article Received*: 05 September 2021*
Revised*: 09 October 2021*
Accepted*: 22 November 2021*
Publication*: 26 December 2021*

Abstract
Modern technology supports network environment success by incorporating numerous networking infrastructure platforms and third-party apps. Data outsourcing, whereby data owners store their own data in a public hub, is a promising advantage. Although obtaining similar data from the storage service is likewise thought to be a difficult task by large service providers, security of that data is a major worry.In this essay, A brand-new procedure termed binary data conversion is suggested to enhance data outsourcing security and boost the effectiveness of retrieving related multimedia documents. To increase search performance in storage services, an encrypted index for video data is developed using the most modern AES algorithm. To enable quick and precise search queries.

Keyword: Advanced Encryption standards, binary data conversion, data confidentiality, data security.

1. Introduction

In ultramodern life utmost of the communication will be videotape grounded and the communication hedge also grown as an arising point to employ more video transfer. Contemporaneously video communication is getting vulnerable to different types of attack over the communication channel. At the time that's same providers solicitations to store their videotape in a garçon for the weal of consumer either by free service or paid services. Storing vids in the garçon that's public considered as further dangerous factor because hackers may thieve videotape at any time. To save the videotape from any attacking service security must be assured at veritably position that's high. To overcome that issue, some of the videotape encryption system should be enforced as well as possible to cipher the videotape before transmission and decipher at the receiver side.

Encryption is a system used to conceal the perceptive information stored in the videotape. Decryption is nothing but restoring the original data from translated data. In different aspect encryption isn't only used for hiding the information from bushwhackers it's also used to view the videotape data in demoralized View and quality that's high can be viewed only by authorized stoner who have proper key for decryption. Cracking mass videotape isn't easy so it must be translated cautiously with different mode. To cipher enlarge videotape, size of the videotape should be reduced, To reduce the size videotape should be compressed before encryption using contraction styles like MPEG 1/2/4,H.263,H.264 Or factor that'sAVC.Important that encryption shouldn't

disturb the effectiveness of compressed video. Binary conversion algorithms are incorporated to enhance the security in videotape storehouse service. Several encryption styles are available in videotape encryption they're picky encryption, Perceptual encryption, Permutation encryption and completely layered encryption etc.

In picky algorithm it shall cipher on the base of four factors like cracking all title part, cracking the all title and I frame, cipher all the I frames like cracking P frame and B frame. also eventually cipher all the frames like naive algorithm to insure security that's high the both the end. Before compressing the videotape aqueducts, the Zigzag Algorithm is utilised to encipher the data on them. To be more specific, the mapping of 8x8 blocks to a 1x64 vector is done again in the same order each time. For the purpose of concealing the transformation of the 8x8 block into the 1x64 vector, a permutation at random is used. The fundamental idea is excluded from the ZIGZAG permutation algorithms. The major drawback is that if a permutation list is discovered, the algorithm will no longer be secure. This renders the technique useless.

A new algorithm known as VEA has been developed for the videotape encryption technique, and it relies on the division of VHS aqueducts into gobbets. These gobbets have been split up into two distinct lists: one for odd, and the other for indeed. After that, applying an encryption technique such as DES to the indeed list and the final cypher textbook is a matter of combining the encryption algorithm XOR with the odd list aqueducts. This is a consecution of affair.

Pure Permutation is simple to apply a permutation fashion for the I frames. Since both the sender and the receiver have only the permutation that's correct encrypt and decipher the videotape aqueducts independently. The entire contents of the videotape are first compressed, and then translated utilising typical convention algorithms such as DES, RSA, IDEA, and AES, amongst others, in the process of completely focused encryption. Due to the extensive amount of math required and the poor speed, this method is not appropriate for real time videotape operations.

The encrypted multimedia data are still only partially recognisable after encryption using the perceptual encryption method, which necessitates that the quality of the audio and visual data be only partially degraded by the encryption process. Additionally, the audio and visual quality declination must be entirely regulated by a factor.

Section ii describes the affiliated work Section iii is about proposed methodology Section iv explains the perpetration Section v reveals about performance measure Section vi conclude the work that's overall

2. Literature Review

John Singh and Manimegalai are the ones who came up with the idea for this paper (3). The author implements a brand new approach that he calls Fast arbitrary Bit Encryption ways (FRBET). First, the videotape is used as an input, and then it is subjected to a lossless compression process in order to minimise the overall size of the videotape so that it may be encrypted more effectively. It is essential that videotape be compressed, as failure to do so will result in a noticeable decline in the

quality of the recording. The algorithm for the advanced encryption standard (AES) is utilised so that the videotape can be encrypted. After that, the key is cut into four sections, and each section is then translated using a different arbitrary integer. Additionally, it is padded with zeroes to boost the critical strength in the event that some of the bits are missing from the 8-bit representation. In addition, in order to avoid problems, the sender and the receiver should each be provided with the same arbitrary critical number. A fixed length of hash data is produced by padding the bit 0's and 1's; the length of the fixed data is determined by the hash function. In addition, it is dependent on the swab algorithm in order to generate swabs for the hash function. Before performing the swab algorithm, the data that has been translated using AES should be transformed into frames. The creation of the essential grounded word results in the generation of the crucial result from swab alg. key is partitioned into four corridors, each of which is then XORed with an arbitrary integer. Additionally, PKCS7 is padded with key in order to generate a protected key function.

In this study (4) by Vino1 and Logashanmugam, a new approach to drop the outflow was proposed. This algorithm conforms to the H.264 standard. It will be protected against cypher textbook attacks exclusively, as well as attacks based on known textbooks, which are straightforward. The error forbearance process begins with the disclosure of the secret elements of the measure that are participated in by AC and DC. It does not help to identify the object that is being stirred if the feting object that it is attached to is full. It's possible that information could be lost through the P and B frames of the I block. This leakage can be stopped by deciphering this I block as well; however, deciphering an I block takes approximately the same amount of time as ciphering those data. It is not appropriate for videotapes or enlargements that are sensitive.

The authors of this study (5) are WANG Li-feng and NIU Jian. Introduced an innovative plan that doesn't require much effort. The Luminance transfigure Measure Encryption algorithm takes advantage of some of the most important aspects of the H.264 standard. In order to provide safety and efficiency while consuming a low amount of power, having a fast processing speed and having bandwidth capabilities in a wireless platform is necessary. Sluice figuring is used to translate the residual data's impact on the overall efficacy. This approach significantly encrypts the luminance transfigure measure as a result of an effect that is more noticeable than the chrominance. Sluice cyphers are more concentrated than block cyphers so that they can avoid errors caused by propagation. The use of a typical encryption algorithm guarantees the user's safety. Changing the value of a certain parameter will result in an adjusted bitrate.

The authors of this research (6), Zhang Qian and Wu Jin, proposed a new encryption technique for the goal of improving VHS conferencing. A novel permutation law and DES algorithm with three different schemes for H.264 norms were both introduced by it. This approach employs the method of cracking a portion of the stir chrominance and vector, as well as the luminance of the residual data from the DCT measure. Additionally, the stir vector is encrypted using intra-vaticination. The I and P frames of the inter vaticination mode contribute to further confusion brought about by the contraindication metaphor encrypting. It has a remarkable slowing effect on the pace of contraction.

In this publication (7), the authors of varalaxmi.l developed a new encryption method for the transmission of real-time videotapes. The primary component of the plan is for videos to be

transformed into DCT measure and then translated through the use of secret sharing. The exchange of secrets is a method that can be used to verify that there is no conformity among the groups that uncover secrets. Using a creator that is completely random, stir vectors are either transformed or scrambled. Coming offer is utilised in order to carry out sea that is divided on the pieces in order to utilise a secret sharing approach. Intra prediction encryption is performed by employing a method known as PRNG in conjunction with the secret sharing of DWT, and it also follows the remainder of the procedure that came before it. The final technique makes use of an algorithm known as According to perform spatial correlation of frames. Additionally, this algorithm is utilised to transform a group of film land into a single group by making advantage of inter-frame redundancies.It defends against attacks using only the cypher textbook and known pain only using the cypher textbook.

This paper (8) Roy and Pradhan Proposed a new videotape encryption algorithm called RVEA, It's principally works on both high resolution vids and normal vids. It consider as that the AES algorithm is effective than DES for crucial security and strength purpose. It originally gives significance to low frequency portions and 128bit encryption is done at bit ofsec. Author believes that though it take number of calculation time it achieves high security and it's well matched alg for peer- peer videotape on demand operation.

This paper(9) Proposes a Layered videotape encryption to distort frames ofH.264 norms to avoid errorpropogation.security and speed is maintained at different situations and encryption is done at three position like base subcaste, middle subcaste and improvement subcaste. At each subcaste encryptions are done at different situations. Only upper portion are translated in base subcaste and deformation is done at nethermost position of intra enciphered frames. nearly 20 of MB are translated. In the middle subcaste it contains sensitive information that lies on I frame, MB’s of base subcaste are translated and centre part also translated. Outflow is high in cracking base subcaste. The entire frames of both intra and inter enciphered frames are translated by improvement subcaste. These subcaste encryptions give further and further security but it takes further cost that's computational it's recommended only for extremely sensitive vids.

This paper (10) proposes a Perceptual encryption for the videotape It doesn't cipher the full layered videotape but it's used to degrade the quality of vids. Low quality videotape can be seen indeed after encryption. This type of scheme is accessible only for the operation like peer- peer videotape and pay scale videotape. Low scale videotape is available for non-outstanding stoner advanced interpretation can be seen by paid stoner. In perceptual encryption a control factor P plays the major part by varying the value of p from(0 to 1) can achieve encryption impact on vids.

3. Proposed Method

3.1 System Architecture

Data proprietor The data owner is primarily regarded as a videotape supplier who saves the data in a garcon. The data is owned by the data owner. Before the data on the videotape is uploaded to the garcon, the provider of the VHS encrypts the data on the videotape. The indication and meta data of

the videotape need to be translated using cryptographic techniques in order to enable secure searching. This can only be done after the tape has been encrypted.

Data stoner The individuals who receive the data after transmitting a translated inquiry to the garcon and then subscribing the videotape data at the stoner end in a secure manner are referred to as data stoner subscribers.

Garçon They are the fundamental garcon that keeps the huge quantity of multimedia stuff that the stoner can subscribe to at any moment without being in danger of losing access to any of it.

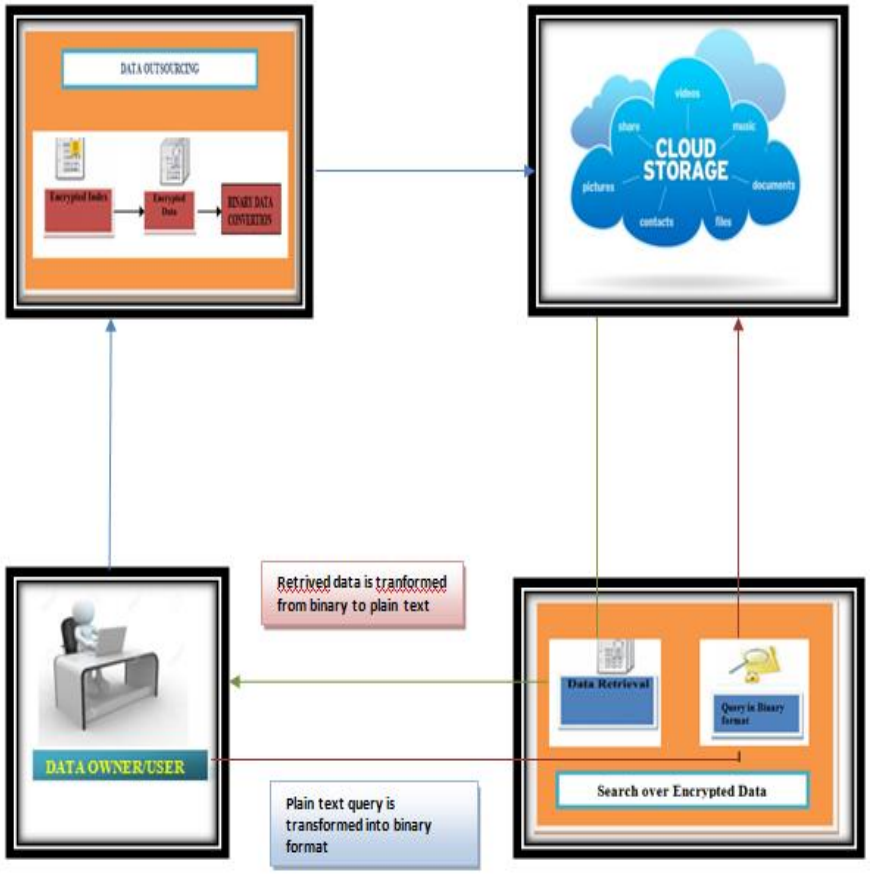
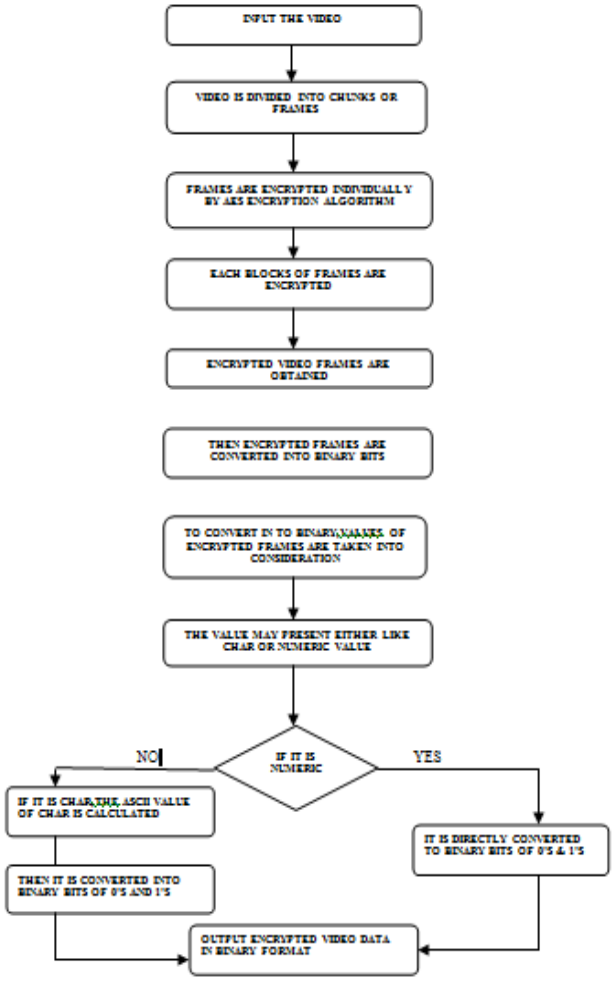


Figure1.System Architecture

3.2 Cryptographic Schemes

Before uploading the video to the server, video provider generates an index for the video for enabling query that is easy and simpler file retrieval. Index should be encrypted before uploading.
Video data=index and meta data.
Generating Encrypted index: Index is considered as the pointer it enables the server to easily recognize which video is subscribed by the user and also insisting file retrieval that is easy. Encrypted index is created AES that is using algorithm.

3.4 Flow chart for proposed methodology



2. Experiment Result:

The trial is conducted on Real time MP4 videotape. A secure videotape transmission is enforced using Windows platform placing garçon and customer at onesystem.It's enciphered by using a utmost programming language java that's ultramodern. To explode real- time communication encryption is done at garçon side and decryption is done at receiver side. By enforcing this algorithm we examined by one frame of the whole videotape. The frame that's original show in fig2.

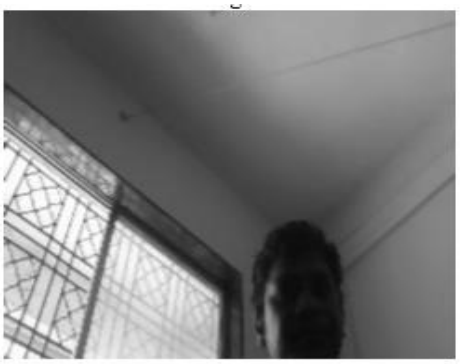


Figure2. Original frame

Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2463

Encryption is done with the DCT measure of sign bits of I frame. by doing encryption on I frame of sign bits we can get the blur image it's showed in the fig3.

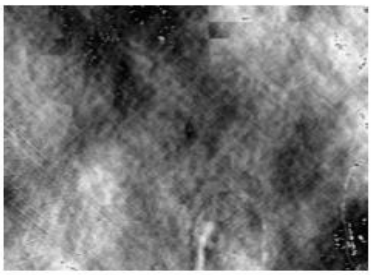


Figure3. Encrypted with sign bits of AC and DC coefficient.

Then the pixel or size that is exact of frame is obtained with number of rows and column representation. It is shown in the fig4.

7	6	5	7	8	5	4	1
7	7	5	7	4	3	1	6
3	2	6	8	9	7	5	7
9	7	5	3	2	1	9	7
5	7	4	1	7	8	0	7
7	3	4	7	5	7	8	2
7	2	7	3	7	5	7	7
3	7	7	2	7	6	1	0

Figure 4 Encrypted frame value

The pixels may be presented either in character or numeric value after carrying the pixels of the translated image. If it's represented in numeric it's directly converted into double value or additional ASCII value of housekeeper is set up and also it's converted into double bits. The bits should be represented with 8bits. The double conversion is done with double data conversion algorithm(BDC) and it's shown in the fig5.

1	0	0	1	1	0	0	0
1	1	0	1	1	0	0	0
0	0	0	1	0	1	0	1
1	1	0	0	1	0	1	1
0	1	0	0	0	1	0	1
1	0	0	1	0	1	1	0
1	0	1	0	1	0	1	1
0	1	1	0	1	0	0	0

Figure 5 Encrypted frame converted to binary bits

5 Performance Analysis

5.1 Comparison of time taken for Encryption by different algorithm:

Encrytpion time is calculated for different encryption algorithm for different multimedia file in different size. It is showed in the fig6.

INPUT FILE	SIZE IN MB	ENCRYPTION EXECUTION TIME IN SEC(MSEC)				
		AES	DES	SDES	TDES	TWOFISH
		128	64	64	168	128
TEXT	12	2580	7500	11000	10200	6000
	24.8	4400	15095	12000	17000	13000
	48	5590	18000	19000	20010	25010
IMAGE	16.9	6000	9500	13000	10520	6200
	26	9400	11400	15300	15400	17200
	55	19002	20003	20500	23100	25200
AUDIO	15.7	3710	6520	10000	8450	9250
	35.0	8100	15200	20100	19000	17150
	71	11240	20520	23470	19100	21000
VIDEO	15	4200	8100	10310	12200	6170
	25	7500	10100	12200	13000	12200
	49	19500	21250	23590	25150	22490

Table1 Encryption computation time

5.2 Decryption computation time

Decryption time is calculated to found how much time is take to convert cipher text to plain text. It is helpful to find the throughput.

INPUT FILE	SIZE IN MB	DECRYPTION EXECUTION TIME IN SEC(MSEC)				
		AES	DES	SDES	TDES	TWOFISH
		128	64	64	168	128
TEXT	12	4580	7500	13000	11200	7000
	24.8	9400	15000	21000	19000	16000
	48	17590	26000	29000	28010	27010
IMAGE	16.9	6600	10500	15000	13520	9200
	26	10400	15400	19300	18400	18200
	55	21002	23003	24500	27100	28200
AUDIO	15.7	5710	7520	11000	10450	10250
	35.0	10100	18200	22100	21000	20150
	71	15240	23520	25470	25100	25000
VIDEO	15	6200	7100	11310	10200	7170
	25	8500	11100	14200	14000	12200
	49	21500	23250	26590	28150	25490

Table2. Encryption computation time

6 Conclusion

The proposed way of securing data in public centres is superior to any other data security measure that was described in the check of the relevant literature. An everlastingly safe Advanced encryption standard fashion has been stationed, and in order to further boost the level of security, the translated data have been converted and saved in a double format at a public centre. The performance is measured to demonstrate that our offer is more important against any cyberattacks, and a comparison table is offered to demonstrate that the AES algorithm is superior to any other algorithms in terms of size and cost in order to guarantee better security. It assures that our product

keeps data confidential while data is being transmitted, and it has been demonstrated that keeping data in double format assists in reacquiring comparable data with a little increase in output.

Reference

[1] Xingliang, Xinyu Wang, jinfan Wang, "Enabling Secure and Efficient Video delivery through Encrypted In-network Caching", in IEEE journal on selected areas in communication, 2016

[2] Qian Wang,Meiqi He,Minxin Du, "Searchable Encryption over Feature-Rich Data", in IEEE Transaction on Dependable and Secure Computing, VOL. 13,NO. 9,Sep 2014.

[3]K. John Singh, R. Manimegalai, "Fast Random Bit Encryption Technique for Video Data", European Journal of Scientific Research, Vol.64, No.3, 2011, pp. 437-445

[4]T. Vino1, E. Logashanmugam, "A Model-based Multimedia Encryption Scheme for Real Time Videos", IEEE International Conference on Recent Advances Space Technology Services and Climate Change, pp. 171-173 ,2010.

[5]WANG Li-feng, NIU Jian-wei, MA Jian, WANG Wendong, XIAO Chen, "A Lightweight Video Encryption Algorithm for Wireless Application", Fifth IEEE International Symposium on Embedded Computing, 2008

[6]Zhang Qian, Wu Jin-mu, Zhao Hai-xia, "Efficiency Video Encryption Scheme Based on H.264 Coding Standard and Permutation Code Algorithm", IEEE World Congress on Computer Science and Information Engineering, 2009, pp. 674-678.

[7]Varalakshmi. L. M., Dr. Florence Sudha. G., Vijayalakshmi. V., "Enhanced Encryption schemes of video for real time", In the proceedings of the International Conference on Signal Processing, Communication, Computing and Networking Technologies, pp. 408-413, 2011

[8]Lei Chen, Narasimha Shashidhar, Qingzhong Liu, "Scalable Secure MJPEG Video Streaming", In the proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops, 2012, pp. 111-115

[9]Lingling Tong, Gang Cao, Jintao Li., "Layered Video Encryption Utilizing Error Propagation in H.264/AVC", In the proceeding of the IEEE Symposium on Electrical & Electronics Engineering, 2012, pp. 182-187

[10]Shunjun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo, "On the Design of Perceptual MPEG Video Encryption Algorithm", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, No. 2, 2007, pp. 214-223

[11]R. R. Igorevich, H. Yong, D.Min, E. Choi "A study on multimedia security systems in video encryption," in proceeding of IEEE 6th International Conference on Network Computing. 2010, pp. 1-5

[12]Shiva Krishna Reddy, k. Srimathi, R. Rajalakshmi," The Indexing Algorithm for scrambled frames in video encryption", International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 4, pp. 651-655, February – 2014.