INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY
Monthly Peer-Reviewed, Refereed, Indexed Journal
Volume - 8, Issue - 1

ISSN(O): 2456-6683
[Impact Factor: 7.148]
January - 2024

IJRCS

DOIs:10.2017/IJRCS/202401021 --:-- Research Paper / Article / Review

Hybridization of Advance Encryption Standard Algorithm and Blowfish Algorithm

Mohan Kumar Patel

Assistant Professor, CSE, Madhyanchal Professional University, Bhopal, India
Email- patel.mohan67@gmail.com

Abstract: *An alternate technique is to scramble the video information utilizing any of the cryptographic encryption calculations. This proposal is an exertion to give answers for the ongoing feature applications, fulfilling the obligations in the current research. In this dissertation AES and blowfish algorithm for video encryption based on random process of password generation have been applied for efficient encryption and decryption process. The data is processed in the form of video file but the file is not processed directly for the encryption and decryption process. So first the whole video is converted into binary file for the encryption and decryption process. Means here the binary data is accepted as the input. The results are compared based on the bin calculation, speed of different algorithms and the encryption time and data loss. The results from the experimentation indicate that the variations in the RGB of original and encrypted image are very high so to decipher it is very tough. The E-time comparison of our approach proof to be useful in comparison to the individual and different states of algorithm used. Data loss comparison shows the minimum data loss in our process so the data loss is less.*

Key Words: *Video cryptography, video steganography, data security, XOR.*

1. INTRODUCTION :

The advancement of Internet over the previous decades has catalyzed the era of expansive amount of advanced media content. The measure of media substance accessible on the Internet is expanding at an exponential rate. With the development in correspondence innovation, ubiquity of sight and sound information has additionally expanded. The advance in media dissemination innovation has brought about simple accessibility of sight and sound substance to different clients over the correspondence channels. Users customers of the mixed media information are presently fit to perform continuous sound and feature conferencing, listen to music, perspective streaming feature cuts and so forth. They likewise perspective movies and news on the World Wide Web (WWW).

Nonetheless, a large portion of the systems utilized for mixed media appropriation is open channels; and, all things considered, they are profoundly unreliable 1. These systems are helpless to assaults, and they are not suitable for transmitting touchy and profitable media substance such as military, monetary or individual features. This requires secure encryption calculations for interactive media information security. The substance maker (stockpiling server) transmits content over the system, and all the clients joined with the system access this substance. Accept Alice needs to transmit certain interactive media information to Bob. In the event that she uses such a system to transmit this substance, all different clients associated with the system separated from Bob can likewise get to this substance. On the off chance that she needs to limit the substance just to Bob, she can utilize verification control instruments. Case in point any one can utilize a private impart along to secret key security.

Then again, applying this system alone is definitely not enough to secure interactive media information telecast over the open-open stations. To empower secure sight and sound transmission over these open channels, we have to encode the sight and sound information before transmitting it. Information encryption is basically encoding the information in such a route, to the point that just approved clients can decipher the content. For all others, the information does not bode well. Encryption calculations have been generally concentrated on for the printed information in the past 2. This has brought about standard calculations like Data Encryption Standard 3., Advanced Encryption Standard 4 furthermore RSA 5. Be that as it may, guide expansion of the calculations to sight and sound does not bring about basically helpful sight and sound encryption plans. All these calculations are composed focused around the text based attributes. We presently clarify why sight and sound encryption will must be not quite the same as text based encryption.

In all of the natural videos, if the video in terms of images have been considered, the values of the neighboring pixels are strongly correlated the value of any given pixel can be reasonably predicted from the values of its neighbors. In this dissertation advanced encryption standard (AES) and blowfish algorithm for video encryption based on random process of password generation have been applied for efficient encryption and decryption process. AES is chosen as it is faster and supports larger key size. Blowfish algorithm is chosen as it is securing the data in 16 rounds and efficient in image encryption. After encryption it is compared by frequency bins in terms of Histogram. Then calculated the information randomness in terms of information loss so that the information loss can be determined.

2. PROPOSED WORK FOR ENCRYPTION AND DECRYPTION :

In this dissertation the combination of AES and blowfish algorithm is applied for data encryption and decryption process. Algorithm 1 shows the whole process of AES algorithm. The binary data is input for the AES and blowfish encryption process. First AES algorithm is applied on the computational bytes. AES used all the 128 bits of a plaintext block as the 16 bytes. The formations of sixteen bytes are process as a matrix of 4*4. The main benefit of using AES is it is variable in nature as it uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds utilizes an alternate 128-piece round key, which is computed from the first AES key. Figure 4.2, 4.3 and 4.4 shows the process, substitution and encryption and decryption process. Figure 4.5 shows the flowchart which depicts the whole process clearly.

Following steps used to encrypt
Proposed algorithm 1 AES and blowfish algorithm
Step 1: Input the binary data as the plaintext.
Step 2: Byte substitution process is applied. The 16 bytes which are imputed are substituted by looking up a fixed table (S-box) in design. It produced the 4*4 matrix.
Step 3: The starting four rows of the matrix is left shifted. The failing bits are shifted to the right side of row.
Step 4: It is used for mixing the columns.
Step 5: It is used for adding the round key.
Step 6: Then key expansion is performed.
Step 7: The computation of subkeys.
Step 8: The encryption face is then started.

The process of decryption of an AES and blowfish is applied in the similar manner of the encryption process but the
reverse order is used. In this the following rounds are used for the data decryption.
Add round key
Mix columns
Shift rows
Byte substitution

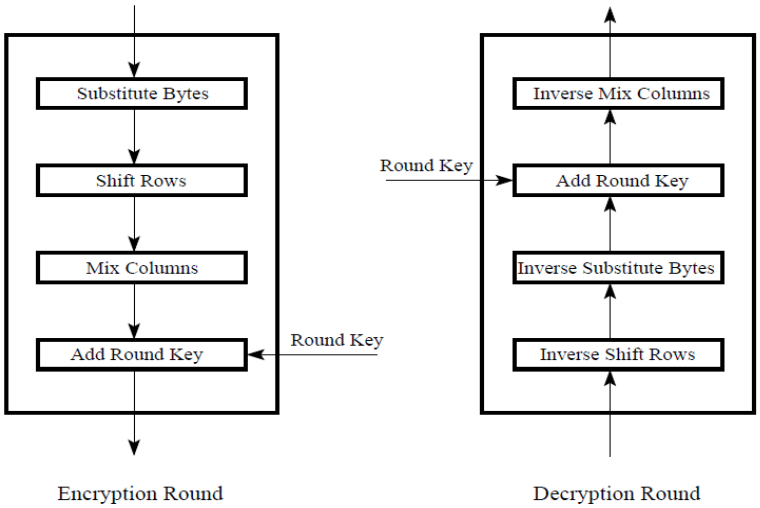

Fig. 1 Encryption and decryption round

Bin calculation

Bins are created based on the same size data groups which including the first and the last part or the max or min participation of the data. A histogram is a plot that gives you a chance to find, and show, the basic recurrence conveyance (shape) of an arrangement of consistent information receptacles. This permits the review of the information for its hidden anomalies, skewness, and so on.

Proposed algorithm 2 Bin Generation

Step 1: The smallest and the largest value are calculated.

Step 2: The values are produced as the round off value with 16 bins. It can vary case by case. In our case 16 bins are considered.

Step 3: Partition your range (the numbers in your information set) by the receptacle estimate you picked in Step 3. For instance, on the off chance that you have numbers that range from 0 to 50, and you picked 5 canisters, your receptacle size is 50/5=10.

Step 4: Make the canister limits by beginning with your littlest number and including the receptacle estimate from Step 3. For instance, if your littlest number is 0 and your canister size is 10 you would have receptacle limits of 0, 10, 20…

Step 5: It is based on the extraction of the RGB values and then mapping is performed for the calculation of the bin distance and summing it

Data loss

Then data loss is checked for the purpose of checking the strength of encryption standard. By this approach data loss information can be checked for the purpose. It is checked for the purpose that for checking the possibility of information loss after encryption and decryption process. It should be minimum so that efficient data retrieval is possible otherwise data retrieval is cryptic [15].

$$\sum_{i=1}^{n} - p(s_i) \log_2 p(s_i)$$

3. OUTPUT AND EXPERIMENTAL RESULT :

Result Evaluation

In this chapter result analyses have been presented based on AES and blowfish algorithm. The results are compared in three different categories. First category compares the data based on the bin calculation. The second comparison is based on the speed of different algorithms and the encryption time. Third comparison is based on the data loss. For the result analysis TABLE I have been considered for comparison.

TABLE I
Video information

S. No	Name	Size in MB
1	Sample1	53.75
2	Sample2	52.24
3	Sample3	41.60
4	Sample4	42.72
5	Sample5	44.04
6	Sample6	25.63

First category compares the data based on the bin calculation. Samples are considered for this experimentation and it is found that the variations in RGB bins are nominal and so that encryption process works

correctly and well suited for the video encryption. It is also clear that the variations in the RGB of original and encrypted image are very high so to decipher it is very tough. E-time comparison is shown the comparison of encryption time from previous method and our approach proof to be useful in comparison to the individual and different states of algorithm used.

Data loss comparison is shown in TABLE II which shows the minimum data loss in our process so the data loss is less.

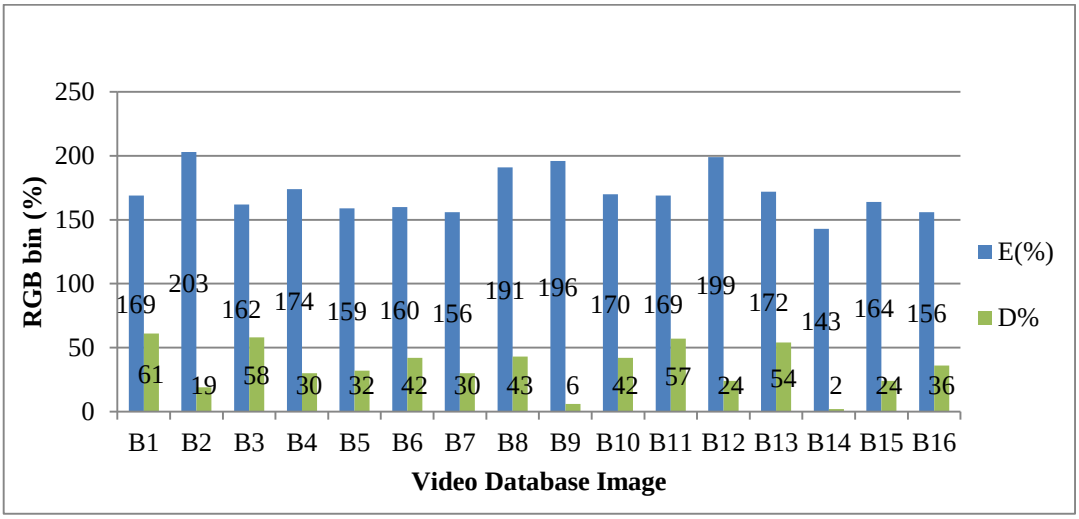

Fig. 3 RGB Bin comparison for video encryption and decryption for sample 1

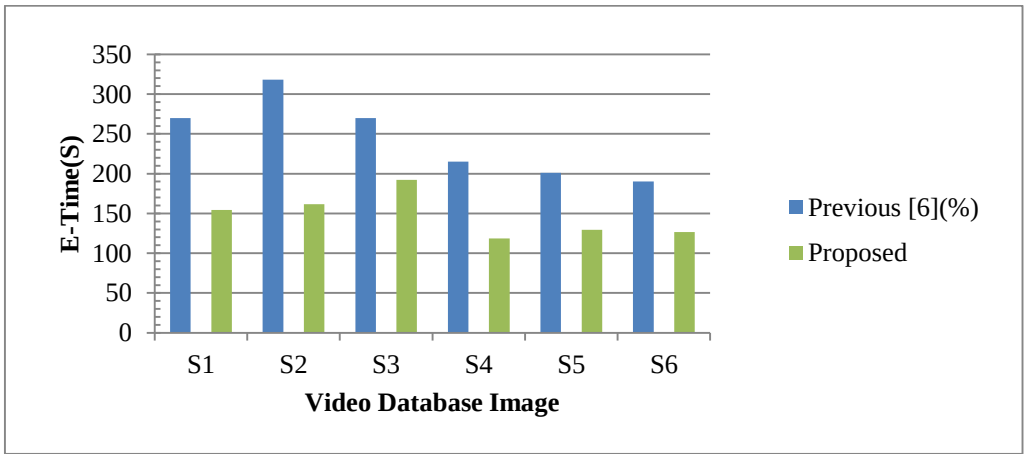

Fig. 4 Comparative graph for encryption time of previous and proposed method for sample 1

TABLE II
Comparative Data loss table of different video samples

S. No	Data Loss
S1	0.28
S2	0.18
S3	0.24
S4	0.29
S5	0.14
S6	0.02

4. Conclusion :

In this dissertation advanced encryption standard (AES) and blowfish algorithm for video encryption based on random process of password generation have been applied for efficient encryption and decryption process. AES is chosen as it is faster and supports larger key size. Blowfish algorithm is chosen as it is securing the data in 16 rounds and efficient in image encryption. The results are compared in three different categories. First category compares the data based on the bin calculation. The second comparison is based on the speed of different algorithms and the encryption time. Third comparison is based on the data loss. It is found that the variations in RGB bins are nominal and so that encryption process works correctly and well suited for the video encryption. It is also clear that the variations in the RGB of original and encrypted image are very high so to decipher it is very tough. E-time show the comparison of encryption time from previous method and our approach proof to be useful in comparison to the individual and different states of algorithm used. Data loss comparison shows the minimum data loss in our process so the data loss is less. Based on the above result analysis the proposed method is found to be useful.

5. Future Work :

- There are several encryption techniques which are already easily applicable on text data and provide better security. In future other encryption standards can be applied so that security mechanism will be improved.
- The size of image is variable and in contrast when it is converted to binary file it is tedious some time to manage the large account of size. So this area is also improved in future.
- In future animation files and flash files are also considered for security.
- Hybrid encryption with chaos system can be applied for better security.
- Data support is also limited it can be extended to all video file format available.

REFERENCES :

1. Jakimoski G, Subbalakshmi KP. Cryptanalysis of some multimedia encryption schemes. IEEE Transactions on Multimedia. 2008; 10(3):330-8.
2. Tan CC, Wang H, Zhong S, Li Q. Body sensor network security: an identity-based cryptography approach. In Proceedings of the first ACM conference on Wireless network security 2008 (pp. 148-153). ACM.
3. Davis R. The data encryption standard in perspective. IEEE Communications Society Magazine. 1978; 16(6):5-9.
4. Chodowiec P, Gaj K. Very compact FPGA implementation of the AES algorithm. In International Workshop on Cryptographic Hardware and Embedded Systems 2003 (pp. 319-333). Springer Berlin Heidelberg.
5. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1983; 26(1):96-9.
6. Dumbere DM, Janwe NJ. Video encryption using AES algorithm. In Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on 2014 Jul 8 (pp. 332-337). IEEE.
7. Spanos GA, Maples TB. Performance study of a selective encryption scheme for the security of networked, real-time video. In Computer Communications and Networks, 1995. Proceedings. Fourth International Conference on 1995 (pp. 2-10). IEEE.
8. Tosun AS, Feng WC. Efficient multi-layer coding and encryption of MPEG video streams. In Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on 2000 (Vol. 1, pp. 119-122). IEEE.
9. Qiao L, Nahrstedt K. A new algorithm for MPEG video encryption. In Proc. of First International Conference on Imaging Science System and Technology 1997 Jul 21 (pp. 21-29).
10. Jun L, LingLing Z, Changsheng X, Hao H. A two-way selective encryption algorithm for MPEG video. In2006 International Workshop on Networking, Architecture, and Storages (IWNAS'06) 2006 (pp. 5-pp). IEEE.
11. Liu F, Koenig H. A novel encryption algorithm for high resolution video. In Proceedings of the international workshop on Network and operating systems support for digital audio and video 2005 (pp. 69-74). ACM.
12. Stanek M, Staneková L. Unpuzzling Puzzle (analysis of a video encryption algorithm). In AINA (2) 2006 (pp. 20-24).
13. Macq BM, Quisquater JJ. Cryptology for digital TV broadcasting. Proceedings of the IEEE. 1995; 83(6):944-57.
14. Shi C, Bhargava B. A fast MPEG video encryption algorithm. In Proceedings of the sixth ACM international conference on Multimedia 1998 (pp. 81-88). ACM.

15. Shi C, Bhargava B. An efficient MPEG video encryption algorithm. In Reliable Distributed Systems, 1998. Proceedings. Seventeenth IEEE Symposium on 1998 (pp. 381-386). IEEE.
16. Shi C, Wang SY, Bhargava B. MPEG video encryption in real-time using secret key cryptography. In Proc. Int. Conf. Parallel and Distributed Processing Techniques and Applications 1999 (pp. 2822–8). IEEE.
17. Mary S, Christal S. Improved Protection in Video Steganography Used Compressed Video Bitstreams. International Journal on Computer Science and Engineering. 2010; 2(3): 2010.
18. Seredynski F, Bouvry P, Zomaya AY. Cellular automata computations and secret key cryptography. Parallel Computing. 2004;30(5):753-66.
19. Pareek NK, Patidar V, Sud KK. Discrete chaotic cryptography using external key. Physics Letters A. 2003; 309(1):75-82.
20. Iqbal R, Shirmohammadi S, El Saddik A. Compressed-domain encryption of adapted H. 264 video. In Eighth IEEE International Symposium on Multimedia (ISM'06) 2006 Dec (pp. 979-984). IEEE.
21. Raju CN, Umadevi G, Srinathan K, Jawahar CV. Fast and secure real-time video encryption. In Computer Vision, Graphics & Image Processing, 2008. ICVGIP'08. Sixth Indian Conference on 2008 Dec 16 (pp. 257-264). IEEE.
22. Rivest RL. The RC5 encryption algorithm. In International Workshop on Fast Software Encryption 1994 (pp. 86-96). Springer Berlin Heidelberg.
23. Dubey AK, Shandilya SK. A novel J2ME service for mining incremental patterns in mobile computing. In International Conference on Advances in Information and Communication Technologies 2010 Sep 7 (pp. 157-164). Springer Berlin Heidelberg.
24. Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. InInternational Workshop on Cryptographic Hardware and Embedded Systems 2004 Aug 11 (pp. 357-370). Springer Berlin Heidelberg.
25. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. In Workshop on the Theory and Application of Cryptographic Techniques 1984 Aug 19 (pp. 10-18). Springer Berlin Heidelber.