ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

Performance Comparison of AES, Blowfish and Sattolo's Techniques for Video Encryption

M S Rohit [1], R Sanjeev Kunte [2]

Assistant Professor, Dept of CS&E, Jain Institute of Technology, Davangere, Karnataka, India

Professor, Dept of CS&E, J N N College of Engineering, Shimoga, Karnataka, India

ABSTRACT: Ease of multimedia storage and transmission systems has flooded the internet and therefore there is a great need for video encryption to preserve confidentiality and digital rights. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. Legacy encryption techniques are not suitable for securing the video given the need to encrypt in real-time. Hence, we introduced the Sattolo's encryption technique for videos in which scrambles the data using a rigorous permutation technique. In this paper, Sattolo's encryption technique is compared with the AES and blowfish algorithms. Different comparison parameters like histogram analysis, correlation co-efficient, entropy and Number of Pixel Change Rate (NCPR) are used to analyze the efficiency of the techniques.

KEYWORDS: Sattolo, AES, Blowfish, permutation, encryption.

I. INTRODUCTION

Extensive use of multimedia in various applications brings serious thought to security and privacy issues today. Data encryption is a proper method to protect data. It is difficult to use them directly in video encryption as video data are often of large volumes and require real time maneuvers [1]. For the digital video data, the major security perils are unauthorized play, forging, and distortion of video by eavesdropper. Another prerequisite is to ensure the video content privacy against unwanted third parties. Conventional approach like AES, DES called naïve algorithm approach in video encryption is straight approach to encrypt whole video data. These cryptographic algorithms [2] are highly secure but not well suited for video encryption as they cannot process the bulky volume of video data in real time. Numerous algorithms on encryption are easily available and applied in information security. These algorithms can be classified into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric key encryption or secret key encryption, only a single key is used to encrypt and decrypt data. The key should be shared prior to communication between entities. Keys play a vital role because if weak key is used in algorithm then anybody may decrypt the data.

Potency of symmetric key encryption relies on the size of key used. For the same algorithm, encryption using longer key is harder to decode than the one done using smaller key. Till now, various encryption algorithms have been proposed and widely used (DES, RSA, IDEA, AES etc.) [3], most of which are used for text and binary data. Simple loom is to encrypt the complete bit stream with a cryptographic algorithm, such as DES or AES. However videos normally possess a large amount of data and require real-time operations. Therefore, taking into contemplation the specific characteristics for resource-limited systems, novel video encryption algorithm need to be developed. For real world applications, a video encryption algorithm has to take into account various parameters like security, computational efficiency, compression efficiency and so on. The most common classification of encryption techniques is shown in fig 1..

Different types of video applications require different levels of security [4]**.** For example, for Video on Demand, low security will be fine, whereas for military purposes or financial information, high level of security is required to completely prevent unauthorized access. Computational efficiency means that the encryption or decryption process should not cause too much time delay, so that the requirements of real-time applications are met. Video compression is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

employed to reduce the storage space and save bandwidth, so that the encryption process should have the least impact on the compression efficiency.

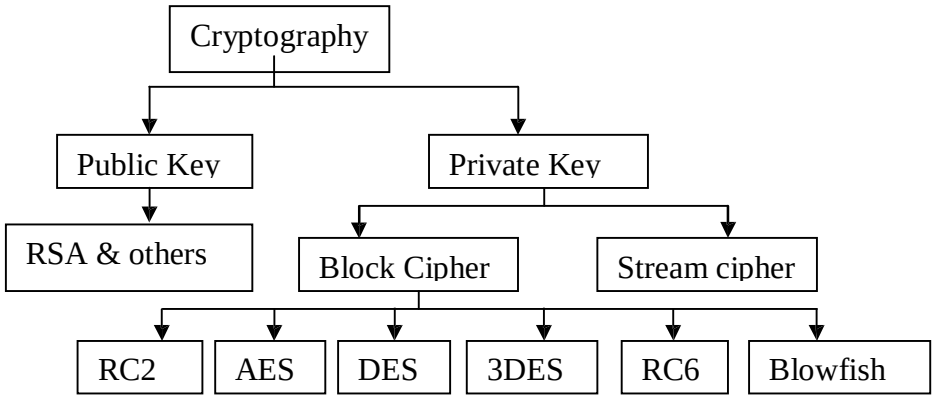

Fig 1: Classification of encryption techniques.

II. BACKGROUND AND JUSTIFICATION

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key size of lengths 128,192 or 256 bits, whereas *Blowfish* is a symmetric block cipher which takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. *Blowfish* was designed in 1993 by **Bruce Schneier** as a fast, free alternative to existing encryption algorithms. Sandro Sattolo published an algorithm for generating uniformly distributed cycles of (maximal) length *n*. Algorithm involved the unique concept of moving the "struck" numbers to the end of the list by swapping them with the last unstruck number at each iteration. A brief overview of three techniques is as shown below:

ADVANCED ENCRYPTION SYSTEM (AES)

AES encryption involves of a series of steps. With the exception of the initial key expansion operation, all the steps are repeated a number of times; each such iteration of steps is called a *round*. The number of rounds used in the algorithm is reliant on the size of the input key. The initial input plaintext data is used to create a matrix of 4x4 bytes of data. The transformed data of this matrix is stored as *state data* during processing of each step. The Key Expansion step expands and transforms a 128-, 192- or 256-bit key to 11, 13, or 15 sub-keys, each 128-bits long, using the Rijndael key expansion algorithm [6]. One sub- key corresponds to each AES processing round, thus each sub-key is referred to as a *round key*. The set of 11, 13, or 15 round keys comprises the *key schedule*. In decryption, the reverse processing steps are used to transform encrypted cipher text to unencrypted plaintext data. This decryption process uses the same key as the encryption process.

The Add Round Key step is a transformation that combines the current state data block and the round key corresponding to the specific round using an XOR function. The Sub Bytes step replaces each state data byte with an entry in a fixed lookup table. The Shift Rows step rotates the four bytes of state data in each row in the state data matrix. The Mix Columns step performs a transformation on the four bytes of state data in each column in the state data matrix.

BLOWFISH

Blowfish uses 64 bits block size, and a variable key size ranges from 32-bits to 448 bits. Blowfish algorithm consists of two parts: key expansion parts and data encryption part. Key expansion converts the key into several sub keys arrays of total of 4168 bytes [7]. Data encryption part is done via 16 round Feistel network. Each round consists of the key permutation and the key and data dependent substitution. All operations are XORs and addition on 32-bit words.. Blowfish uses round keys; the entire contents of all the S-boxes are created by multiple iterations of the block cipher. This enhances the security of the block cipher, since it makes exhaustive search of the key space very difficult, even for short keys.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

SATTOLO'S ENCRYPTION

Sattolo's encryption technique generates a random number such that the 'rand' points to a position in between the first and second last number of the plain text. When the number is 'struck' it is considered as the successive content of the cipher text and the last number in the plain text is placed at the 'struck' position. This forms one round of the encryption technique. The number of rounds is solely dependent on how big the data is, thus making it complex to decode as the data grows in size and vice versa. The block diagram of the Sattolo's encryption is shown in fig 2.

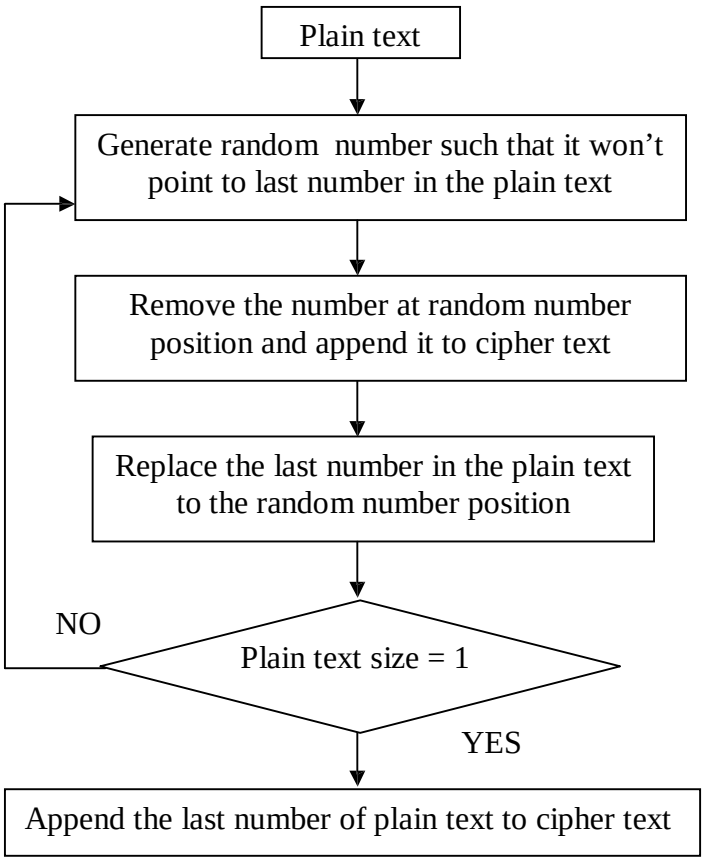

Fig 2 : Sattolo's encryption technique

The Sattolo's technique is mainly based on the permutation demands to be evaluated with the standard, legacy techniques in the field of encryption. Sattolo's encryption employs a unique way of scrambling the plaintext without drawing any suspicion of the eavesdropper. The less time consumed by the Sattolo's technique along with many other parameters are to be compared with the AES and Blowfish.

III. EXPERIMENTAL SETUP AND SIMULATION

This section details the results of the simulation as per the experimental setup. For our experiment, we use a desktop with i3, 2.25 GHz CPU and the java programming language. We considered a random frame from the encrypted and decrypted video for the comparison. Characteristics like time taken to encrypt and decrypt images, entropy, Number of Pixel Change Rate(NCPR) and correlation coefficient are used for comparing the techniques. In addition to these, the histogram is analyzed for the original, encrypted and decrypted images of the three schemes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

TIME, ENTROPY, NUMBER OF PIXEL CHANGE RATE (NCPR) AND CORRELATION COEFFICIENT

The AES and Blowfish techniques work on the bytes of the input plain text whereas the Sattolo's encryption is a permutation technique which scrambles the data row by row when an image is compared. The time taken by Sattolo's encryption is slightly larger than other two techniques. Table 1 shows the time taken to encrypt and decrypt the images, entropy, NCPR and Correlation coefficient using the three techniques. Entropy is defined as the amount of information which must be coded by the compression algorithm.

Table 1: Time taken to encrypt and decrypt the image, Entropy, NCPR and Correlation coefficient

Parameter	Sattolo's algorithm	Blowfish Algorithm	AES algorithm
Time taken for encryption	0.375	0.063	0.147
Time taken for decryption	0.216	0.016	0.029
Entropy	7.8747	7.9963	7.9988
NCPR	99%	99%	99%
Correlation Coefficient	0.0020	0.0050	0.0011

NCPR is used to measure the effect of one pixel change on the entire image. Correlation coefficient is the correlation of two adjacent pixels which is given by covariance divided by the product of the standard deviations.
As per the entropy the values shown in the table, there is no much difference in the information embedded in the encrypted images of the three algorithms. The NPCR values obtained are same for all the three encryption schemes thus all the three are successful in preserving the confidentiality of the data. Correlation coefficient near to zero implies that the original and encrypted data are totally different. As per the obtained values the Sattolo's encryption falls in between the AES and Blowfish techniques

HISTOGRAM ANALYSIS

Frequency distribution shows how often each value in a data set occurs, thus histogram analyses is carried out to check how much suspicion the encryption technique draws. The histogram of the original, encrypted and decrypted images is shown below. Figure 3, 4 and 5 shows the histogram of Sattolo's and Blowfish and AES encryption and decryption respectively.

Fig 3(a) Sattolo's encryption

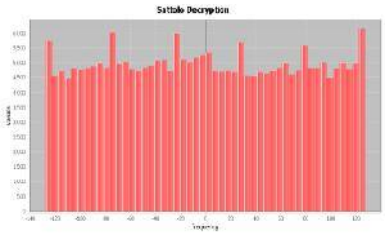

Fig 3(b) Sattolo's decryption

The histogram of the encrypted image does not show frequent variations of the peak levels, hence it does not reveal much information. As it can be seen from the decryption histogram, it doesn't vary a lot compared to the encryption, because Sattolo's technique does not use any substitution boxes and it is a permutation technique which scrambles the content of the image.

But the histogram of the blowfish encryption shows a little variations compared to the sattolo's technique because the Blowfish does not the place the same content in the encrypted image. The substitution is complex, and efficiently helps to conceal the data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

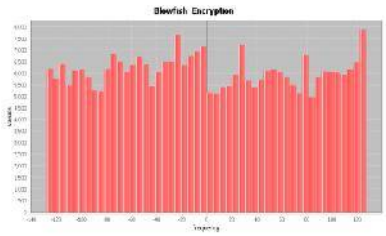

Fig 4(a) : Blowfish encryption

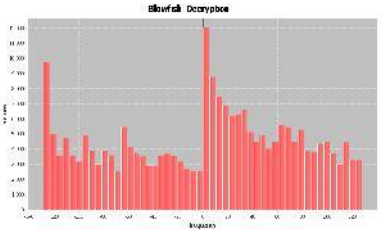

Fig 4(b) : Blowfish encryption

But when compared to the AES technique, the results in the table above show that it is most efficient technique of all. The histogram has fewer variations compared to the blowfish technique. The S-box used in the AES technique replaces the original content with values in the S-box.

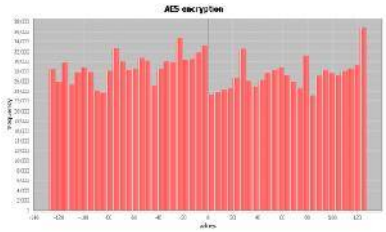

Fig 5(a) AES encryption

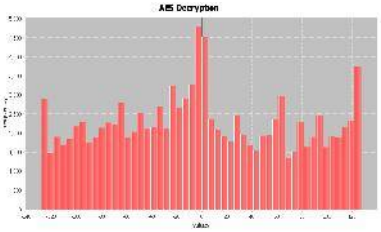

Fig 5(b) AES decryption

Encrypted Images

Sattolo's encryption mainly relies on permutation and thus scrambles the pixels across every row in the image, but substitution has been a key part where AES and Blowfish techniques stand apart from other encryption techniques. A random frame from the input video is chosen and its corresponding encrypted image for the three discussed techniques i.e., Sattolo's, AES and Blowfish are shown in the fig 6(a), 6(b), 6(c) and 6(d) respectively. It is evident that Sattolo's, AES and Blowfish techniques justifies that the permutation must be supported with substitution to avoid identification of original image.

Fig 6(a) Original Image

Fig 6 (b) Sattolo's encryption

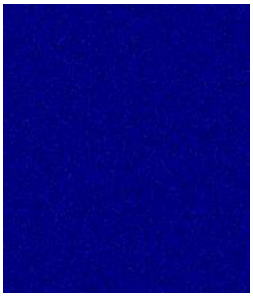

Fig 6(c) AES encryption

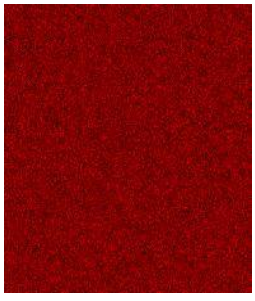

Fig d) Blowfish encryption

IV. CONCLUSION

In this paper we have presented a brief overview of AES, Blowfish and Sattolo's encryption technique. Further, the detailed comparison between the techniques using the time, entropy, NPCR, entropy and histogram as parameters is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

presented. The AES and Blowfish algorithms take very less time compared to Sattolo's technique which draws attention on the complex assignments and replacements done in the Sattolo's technique which consumes more CPU cycles making it a lengthier process. Number of Pixel Change Rate remains same in all the three cases so none of them reveal the identity of original information. Entropy of the AES and Blowfish is higher than the Sattolo's is mainly because of the dense S-box used in those algorithms. The correlation coefficient of Sattolo's scheme is lower compared to the AES and Blowfish hence, the adjacent data are not related to each other, hence it draws less suspicion. Histogram analysis shows that the AES and Blowfish encrypted have some variations in the peak values compared to Sattolo's technique. Sattolo's technique is promising, but it needs lot of improvement when compared to time taken for encryption, which is a major issue in real time applications.

REFERENCES

[1] Sattolo's algorithm (1986), retrieved https://en.wikipedia.org/wiki/FisherYates_shuffle.
[2] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering vol 1.no 2, pp.6-12, 2011.
[3] P. C. Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES , 3DES , AES and Blowfish," vol. 3, no. 8, pp. 6–9, 2012.
[4] Pranav Aggarwal, Skanda Vishwanath, " Design and implementation of video encryption for multi – Media applications", International Journal of Engineering Research and Applications, vol 4, No 4, pp.no 29,34, 2014.
[5] M S Rohit and R Sanjeev Kunte, "A lightweight video encryption scheme based on Sattolo's Permutation technique", Australian Journal of Wireless technologies, Mobility and Security, 2015, vol 1, no 2, pp no 67-70, 2015.
[6] Meredith Lucky, "AES Encryption and CAST's AES IP Cores", CAST, Inc, 2008,
<http:// http://www.cast-inc.com/ip-cores/encryption/cast-AES-IP-overview>.
[7] Pia Singh, "Image encryption and decryption using blowfish algorithm in matlab", International Journal of scientific and Engineering research, vol 4, No 7, pp no 150-154, 2013
[8] M. Abomhara, O. Zakaria, and O. O. Khalifa, "An Overview of Video Encryption Techniques ", International Journal of Computer Theory and Engineering, vol. 2, no. 1, pp. 103–110, 2010.
[9] S Pavithra and E Ramadevi, "Performance Evaluation Of Symmetric Algorithms,", Journal of Global Research in Computer Science, vol. 3, no. 8, pp. 43–45, 2012.
[10] Jolly shah and Vikas Saxena, " Video Encryption : A Survey ", International Journal of Computer Science Issues, vol. 8, no. 2, pp. 525–534, 2011.
[11] S. Sharma and P. K. Pateriya, "A Study Based on the Video Encryption Technique", International Journal of P2P Network Trends and Technology, vol. 3, pp. 40–45, 2013.
[12] S. Gupta, Lalit Kishor and Dinesh Goyal, "Comparative Analysis of Encrypted Video Streaming in Cloud Network", International Journal of Computer Science and Information technologies, vol. 5, no. 4, pp. 5470–5476, 2014.
[13] J. Rajpurohit, Shweta Sharma and Bhagyashree Naruka, "A Comparative Study of Video Encryption Schemes", International Journal of computer Applications vol. 91, no. 4, pp. 10–16, 2014.