Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT TECHNIQUES FOR SECURING DIGITAL VIDEO DATA

[1]ROOPALAKSHMI S, [1]ROSHNI PORWAL, [2]K. JOHN SINGH, [3]R. MANIMEGALAI
[1]School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India
Tail Nadu, India
[2]Assistant Professor (Selection Grade), School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu, India
[3]Professor, Department of Computer Science and Engineering
Park College of Engineering and Technology, Coimbatore, Tamil Nadu, India

E-mail: johnsinghaj@yahoo.com , roopa_snair@yahoo.co.in , roshni.porwal20@gmail.com

ABSTRACT

With fast developments in digital media and communication, transmission of video data over Internet is unsecured due to various security threats. Digital video should be encrypted using any of the cryptographic methods in order to prevent security threats. Cryptography is used for encrypting and decrypting the digital data. Traditional cryptographic systems are often not enough for fast transmission of huge volume of data. In this paper, we study various video encryption mechanisms and analyze their performance. This paper also proposes a new technique called Enhanced Frequency Domain Scrambling Approach (EFDSA) for encrypting video data. Our analysis and experimental results obtained show that the proposed method has less computational overhead and execution time.

Keywords: *Enhanced Frequency Domain Scrambling Approach (EFDSA), Cut and Rotate Technique, Transform Domain Scrambling, Codestream Domain Scrambling, Intra Block Shuffling.*

1. INTRODUCTION

Privacy is a keystone of our ethnicity and is essential in many communal functions. However, our privacy is interfered by modern technologies and security threats. Lot of threat mitigation schemes are available in the literature in order to prevent security threats. Secured video data transmission gains popularity recently due to its huge size. Basically, there are two types of videos, analog video and digital video [1]. Video signal transferred by an analog signal is called analog video. Analog signal may be carried in three ways, namely, composite video format, S-Video and component video format. When one channel is used for transmitting analog video signal, it is known as composite video format. When two channels are used for transmitting analog video signal, it is known as S-Video (Separate Video). When multi channels are used for transmitting the analog video signal, it is called Component Video format.

A digital recording system that works by using digital signals rather than the analog signals, is called Digital Video. There are several advantages of digital video over analog video. Some of them include ease in sharing and storing, high data quality, inexpensive and capacity for multicasting. Video security is achieved by two techniques, namely, Cryptography and Steganography. In cryptography, data is encrypted into unreadable form. The art of protecting information from uninvited individuals by converting it into the unreadable format is called Cryptography. The main aim of this technique is to secure video data from unauthorized person. The process of converting the original video into unreadable video or incomprehensible video is called Encryption [2]. The process of converting the encrypted data to original data is called decryption. The original data transferred or stored, that can be readable by machine or human is called Plaintext. The encrypted data that cannot be readable by human or machine is called Cipher text.

A system that provides encryption and decryption is called Cryptosystem. This system uses algorithms for encrypting and decrypting.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Encryption algorithm shows the simplicity or complexity of the encryption process. In 19th century, a well-known theory was proposed by Kerchhoff regarding the security principle of encryption system. Kerchhoff observed that the encryption algorithm may be known to the opponents, so securing video should be totally rely on the encryption key rather than the encryption algorithm. The key is the piece of information used for encrypting and decrypting the video. The strength of the encryption process is totally depending on the length of the key used. There are two types of cryptographic: i) Encryption and decryption uses the same key ii) techniques that use different, but related keys for encryption and decryption [1]. For encryption and decryption we use same key (secret key) in algorithm is called symmetric algorithm and the algorithms that uses the different keys such as private and public key for encryption and decryption is called asymmetric algorithm.

The process of dividing the video files into small frames is called Scrambling. It is the simplest form of encryption. The domain for analyzing the video signal based on the frequency is called frequency domain. The process of scrambling videos is done according to the frequency range in Frequency Domain Scrambling technique. In this paper we propose an enhanced frequency domain scrambling. Video data is scrambled into frames using some algorithm. These frames are then shuffled and the shuffled frames are encrypted using seed value. The encrypted frames are transmitted over the network with key (public or private). The receiver receives the encrypted frames and decrypts it using the proposed algorithm.

2. RELATED WORKS

The main usage of this scrambling process is in the television industry and the online music market. In TV lines, the video signals are scrambled by inverting the TV lines, moving it backward and forward into the line blanking period, and cutting and rotating the segment of the TV lines [3]. Though re-ordering of TV lines is possible, re-ordering of sample within the TV lines causes certain effects, because while scrambling or descrambling, the samples get affected. Hence descrambling of this video gives flickering effects. Hence, all of these scrambling methods are exemplified as time domain scrambling methods.

The present invention provides the method of scrambling of television signals in frequency domain. According to the preferred incarnation of information a secure scrambling method is provided. This method starts by taking the Fourier transform of the video waveform, V (t) i.e. transforming the signal from the time domain into the frequency domain.

The frequency domain in signal consists of two parts, its magnitude and its phase. The information extracted from the Fourier transform by taking its modules are called magnitude information and the information extracted by taking its arguments are called phase information. There are two degrees of freedom available for the user in video scrambling in the frequency domain; the magnitude attribute may be altered or the phase attribute may be altered.

To deal with the complexity concern, in [4] proposing the Domain Cosines Transform (DCT) coefficient is based on MPEG transmission system. This technique is very easy to implement and changes the statistical property of the DCT coefficients. As a result, it may increase the bit rate of the compressed video by 50% or less. This approach although may not be agreeable to secure transcoding. Another scheme is proposed in which we are permuted to use the line of wavelet coefficients [4].

In wavelet based system, the input video frames are transformed using wavelet filter banks. Here the filtering is done on vertical and horizontal directions. The subband is arranged in spatial arrangement of the original data.

At present, in many places video surveillance system has been used for many purposes. People use this system for monitoring on security purposes. But at the same time the privacy of the data will be lost. Frederic and Touradj [8] proposed a scrambling technique using inverse sign bit of coefficients using Pseudo Random Number Generator (PRNG) and Kenichi et al, proposed the watermarking technique for scrambling. Makoto Takayama et al [4] proposed a new technique with inter block shuffling of AC components, intra-slice shuffling for DC components and intra block shuffling of AC components.

Fredericand Touradj presented a scrambling technique in two steps; transform-domain scrambling using PRNG on DCT coefficients and codestream-domain scrambling applied using Variable Length Code (VLC) process [8].

Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The scrambled codestream are transmitted over network independently with their access rights. Un-authorized person who do not acquire the secret key can only view the hazy version of the content where the privacy of data is concealed. This scrambling process is flexible because the noise inserted can be modified from blurry to very noisy.[6]

In Transform Domain scrambling technique, the MPEG-4 is considered more as it prevails its standard in current video surveillances equipments. However, this approach is directly extensible to all transform-coding technique based on DCT [6]. MPEG-4 is based on a Motion-Compensated (MC) block-based DCT. In this, the frames are coded as intra-frames, predictive – frames and bidirectional frames. In all cases, each frame is divided into 16x16 Macro Blocks (MB). Now this MB consists of four 8x8 luminance blocks and then two 8x8 chrominance blocks, ensuing in 64 DCT coefficients (1 DC and 63 AC coefficients).

On the quantized DCT coefficient, the scrambling process is applied and also to the outside of Motion compensated loop. At the decode side, authorized users perform the unscrambling process to the scrambled data. As shown in the Fig. 1, in MC prediction loop the unscrambled data are used for encoding process. On the contrary, the un-authorized person can also get the video except for the scrambled frames. The main challenge in MC prediction loop is that the un-authorized person should decode both the ROI and the background.

The scrambling process is based on a Pseudo Random Number Generator (PRNG) initialized by a seed value in which many seeds can be used to fortify the security. In this process, video is scrambled into many parts as given by seed value. The authorized person can unscramble this scrambled data using the sequence of seed values. After receiving the scrambled data, authorized person can descramble it and then can decrypt those unscrambled data. For the un-authorized person it is negligible to get the right sequence of seed values.

The main drawback of this technique is that the un-authorized person has negligible chance to access the data. But the radical drawback is that how big the seed values are, more the encryption and decryption process gets complex. So the process overhead increases.

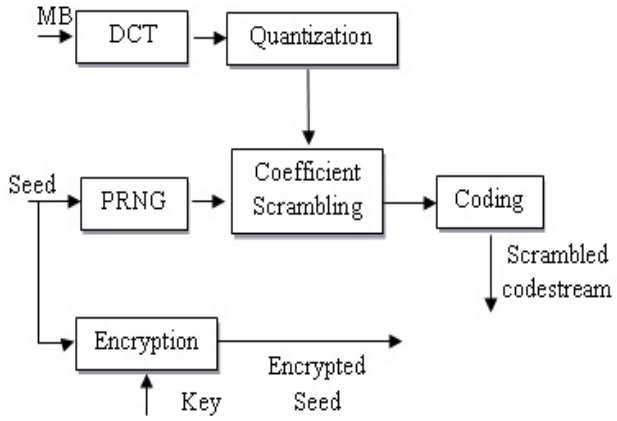

Fig. 1: Region-Based Transform-Domain Scrambling

In Codestream, the AC coefficient of the scrambling process should not have a negative impact on coding efficiency. DC coefficients are strongly correlated with AC coefficient. The amplitude of AC coefficient is interconnected, but their signs are not. By restricting the ac coefficients the scrambling amount can be adjusted, as revealed in the Fig. 2.

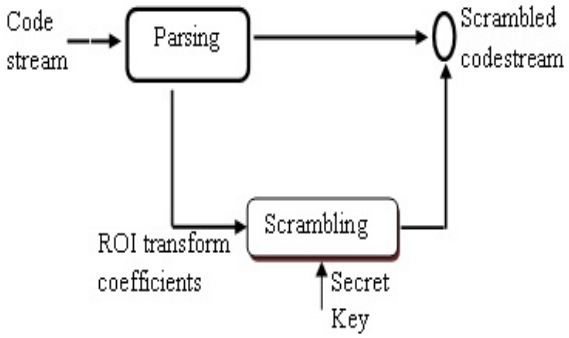

Fig. 2: Codestream-Domain Scrambling in MPEG-4 - Transcoder/Scrambler

The AC coefficient provides sufficient level of concealment. In case the stronger scrambling is needed, DC coefficient is used. In Fig. 3, the scrambling is done by pseudorandom altering the quantized DC coefficients. Here, DC scale is the scaling factor for DC coefficient.

Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

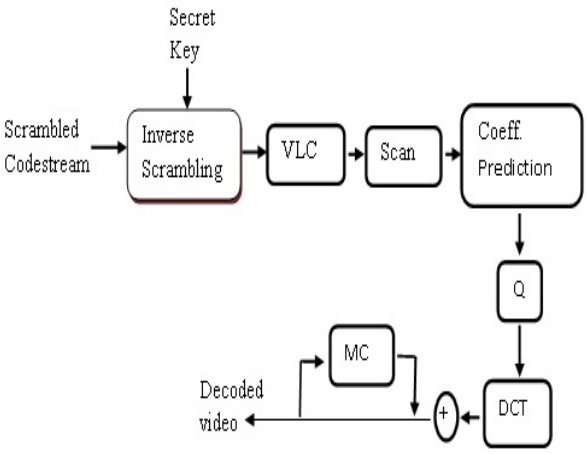

Fig. 3: Codestream-Domain Scrambling in MPEG-4 - Decoder/Unscrambler

The real video is captured (in left hand side) and the video is scrambled and encoded (in right hand side). As shown in Fig. 4, the scrambling process uses the transform domain approach where 63ac are pseudo randomly scrambled. In this process both the pedestrians and the car are successfully scrambled.

Fig. 4: Example of Scrambled Data [8]

Rajat Goel et al proposed a technique in which the moving objects are removed from input picture. The eliminated parts are compressed to JPEG. This image is encrypted by giving password by AES. In an input image the moving objects are masked by erasing/scrambling. This masked picture is transformed by the Discrete Cosine Transform (DCT) and the data objects are encrypted and implanted with the DCT masked image [7].

In scrambling method, all pixels in the moving objects region are randomly permuted. Let there are M objects in the moving object region. Assume $R(i)_{(i=1,2,.....,M)}$ be a generated random number and $p(i)_{(i=1,2,.....,M)}$ is the i^{th} pixel in this region. Then the i^{th} replaced pixel is obtained by permutations is defined as:

$$P(i)=P(R(i))$$

In the erasing method, rousing objects are made invisible. The moving object pixels in an input image are replaced by the same coordinate of the background image pixels. To illustrate the shape of heartrending objects, the edge of the moving objects is unequivocally drawn. First input image is divided into Minimum Coded Unit (MCU). The size of Minimum Coded Unit is 8X8. If the MCU includes the moving objects region then the MCU is compressed by JPEG. A bit stream generated by JPEG is stored in M byte length denoted by array $MO[i]_{(i=1,2,.....M).}$ MO[i] is encrypted by AES and it becomes $MO[i]_{(i=1,2,.....M)}$. For this, first we obtain the scrambling image for DCT coefficient using JPEG technique [9]. We use DCT coefficient of middle frequencies for watermarking. JPEG decoder decodes quantized data because any changes of low coefficient are noticeable and the changes of high coefficient of data lead to immense changes [9].

Decrypting or reconstruction, the encrypted data is extracted from DCT coefficients [9]. Then they are decrypted by using AES. And then the moving objects are recreated with the JPEG decoder. Finally, the recreated moving object is overwritten, in the place of moving object.

Some of the techniques used for scrambling video are: Selective bit scrambling, block shuffling, block rotation, line inversion, sync suppression, line shuffle and cut and rotate. The selected bits in the transform coefficients are encrypted. Here each bit of a coefficient can be examined as one of the three types. Consequence bit of value 1 are the most significant bit, and the value 0 for foregoing bit. Refinement bits are the

Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

remaining magnitude bits, used to refine the coefficient within the known range. The positive or negative is known by the sign bit.

Block shuffling is proposed to increase the level of security. In this method we divide each subband into different blocks**,** as shown in Fig 5. The size of this block may vary for different subbands. In this, for each subband the table generated with the key.

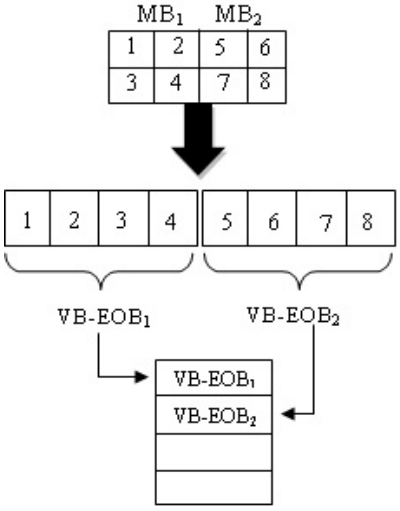

Fig. 5: Intra Block Shuffling [12]

Tfighe blocks of the coefficients are shuffled according to the subband table. At the same time the shuffling of tables is done in different frames. So it may vary from table to table. To increase the security level high we use block rotation. In this rotated block are then encrypted [10]. Thus the level of security increases. Thus it provides more security compare with other types. But in this type the main drawback is that more steps are used for encrypting the data so that the system overhead increases.

In line inversion video scrambling the whole or some parts of the signal scan lines are inverted. This scheme is comparatively cheap and simple to implement but the security level is low. Another method Sync Suppression video scrambling, the horizontal / vertical line syncs are hidden or entirely removed which is shown in Fig. 6. This offer low-cost solution to encryption and also provide good quality video decoding. A typical disadvantage is that the level of darkness reached by this scheme depends on the video content.

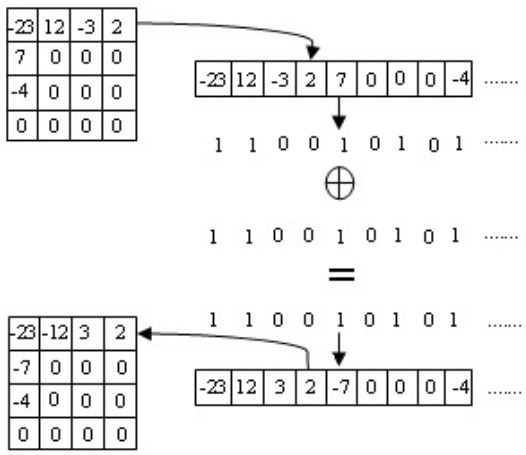

Fig. 6: Synchronous Video Encryption Algorithm [11]

As shown in Fig. 7, In cut and rotate method, each scan line is cut into pieces and then re-assembled in a permuted manner [10]. It provides good quality of video as well as an excellent amount of obscurity and good decode. But the main disadvantage is it needs specialized scrambling equipments.

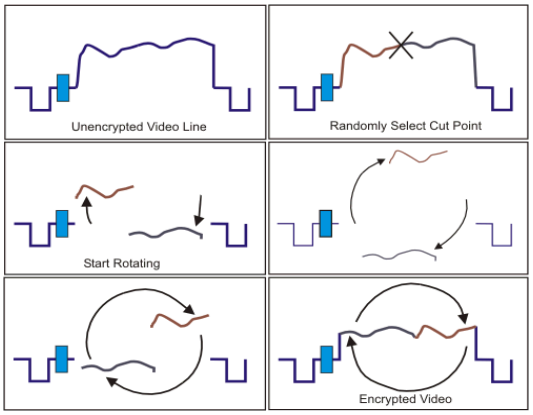

Fig. 7: Cut and Rotate

2.1 Analysis

In the above mentioned techniques the cost analysis is based on two sides basically. The cost required to encode the data as well as the cost required to decode the encoded data. The technique block shuffling in this selection of blocks does not require any extra cost. At the same time the rearranging of these blocks requires little more outlay, as the rescheduling of the blocks. The next technique is block rotation that in comparison with block shuffling it provides

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

good security but at the same time the blocks are rotated using algorithms. Another technique is cut and rotate, in which the video data have been cut randomly as more efficient equipment is needed to cut and rotate it. At the same time on the other end, decoding of these types of data require more computation time.

The security for the process of scrambling can be examined as: For the encryption of the sign bits, the code-breaker is to decode the encoded code for 2^N times, where N is the non-zero coefficients in the frames. If the attacker uses a smoothness constraint to search for the paramount estimate, then this attack will be costly for the attacker. Hence the possibilities of hacking this type are comparatively less. Another step, block shuffling, will render a completely unintelligible image. Theoretically it is difficult to recover the image frame, lacking of knowing the shuffling which mull over a subband that contains 64 blocks.

3. ENHANCED FREQUENCY DOMAIN SCRAMBLING APPROACH

The main aim of our technique is that to provide good security with flexibility. In this, the security of the video is totally based on the sensitivity of the video. If the video is too sensitive and need more security than also our technique will work or else for low security also it will work.

In lower level also our system provides good security. In this, the sender can choose the level of security with the requirement of equipments. There are mainly four levels in our technique.

Level 1: Scrambling the video into frames

In this process, video are scrambled into frames. Using the required algorithm these scrambling process can takes place.

Level 2: Shuffle frames

In this process, the scrambled video (Frames) are shuffled. Here we provide the level of security to the sender. That sender can take the complex algorithm or simple algorithm to shuffle the frames.

Level 3: Encrypting the frames with seed value

Here the shuffled frames are then encrypted with seed value. We provide the flexibility of choosing the seed value to the sender. As according to the sensibility of the data the seed value may change. As if the video is too sensible then the seed value may be large.

Level 4: Pass it key

Afterwards these encrypted frames are then passed on the network with the key (Public / Private). If the network is comparatively safer then public key can use or else private key can use. As here also we are providing the flexibility to sender according to the network through which these data are passed.

In our proposed system, the lower level also provides good security. And here the main advantage is that there will be a good control over the cost and also the system overhead.

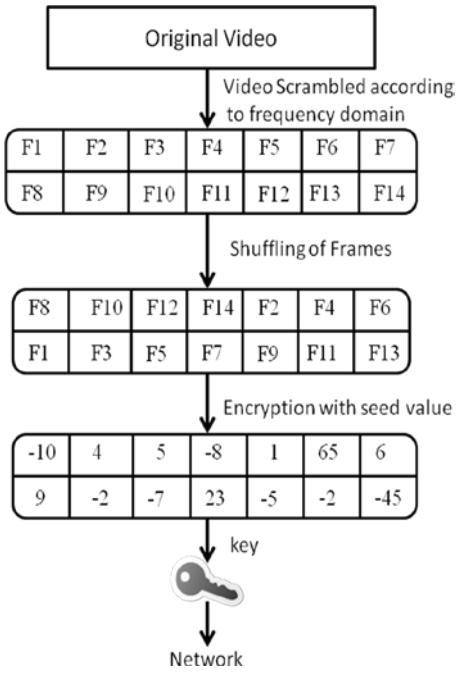

Fig. 8: Proposed System - Sender Side

Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

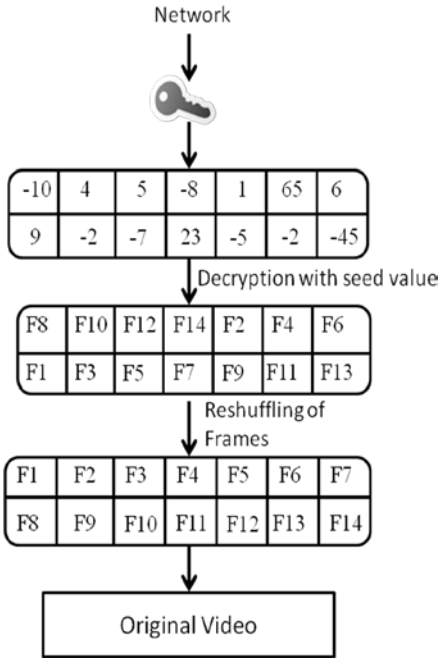

Fig. 9: Proposed System - Receiver Side

In the above figure, the simplest way also provide the better quality of security, as there are four levels. If unauthorized person want to hack, then they should know the values for all four levels. Then only they can access the video. Thus we provide better security at lower level also.

The main advantage of the proposed system is that it provides full control over the cost overhead as well as system overhead. The cost of transferring video data is based on the sensitivity of data. At low level also it provides good security.

4. RESULT

The proposed technique provides good security in low level also. The level of security is totally depends on the sensitivity of the video we passed. The below graph illustrate the comparison between the proposed technique with the existing technique.

The upcoming graph shows how the cost and security varies according to the technique used. The Line Inverse technique use less amount of cost but provide low security level. At the same time the Block Shuffle use more than the LI and also provide less security comparatively CR.

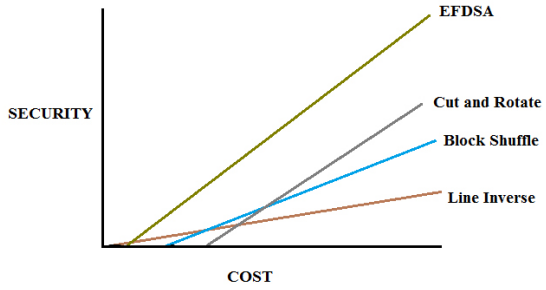

Fig.10 Security and Cost analysis of existing and proposed technique

	Line Inverse	**Block Shuffle**	**Cut and Rotate**	**EFDSA**
Cost	Cheapest	Cheaper than CR	Costly	Flexible
Execution Time	Less	More than LI	More than BS	Flexible
Speed	Fast	Slow than LI	Slowest	Better than CR
Quality	Less	Compatibly good	Good	Good
Space	Less	More than LI	Huge	Flexible
Security at Low level	Worst	Bad	Good	Best
Security at High level	Good	Good	Best	More than CR

Table. 1: Comparison Between Existing And Proposed Technique

- CR- Cut and Rotate
- LI – Line Inverse
- BS – Block Shuffle
- EFDSA – Enhanced Frequency Domain Scrambling Approach

According to the Security level the size of the encrypted data will amend. At the same time the decrypted data quality can also be measured. The comparison is shown in the above table. The fact used in that table is approximate.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSION

The encrypting and decrypting of video is complex due to large file size. There are so many techniques constructed for transferring video data. They all have their own pros and corns. If we take the block shuffling technique the security totally depends on the number of blocks used as well as the way of shuffling. This also creates problem for both the time and overload.

To avoid this we may amend this technique as according to frequency of the video, the scrambling process takes place. And then these scrambled data are then encrypted using any algorithm and passed it to network with key value as private to receiver. This increase the security level as even the sender can't able to decrypt the data. Here the security level takes place in three fields. As first the data are scrambled and shuffled and then these shuffled frames are then encrypted (using some common algorithm known by sender and receiver), then these encrypted data is attached with the private key. So here if video is too sensitive then these three levels should take care. Otherwise according to the importance of the video, the level of security my increase or decrease. Thus the sender has the control of system overload and execution time.

REFERENCES:

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

[2] M. Abomhara, Omar Zakaria, Othman O. Khalifa, "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp. 103-110, 2010.

[3] Jolly shah and Dr. Vikas Saxena, "Video Encryption: A Survey", International Journal of Computer Science, Vol. 8, No. 2, pp. 525-534, 2011.

[4] Makoto Takayama, Kiyoshi Tanaka, Akio Yoneyama and Yasuyuki Nakajima, " A Video Scrambling Scheme Applicable To Local Region Without Data Expansion", In Proceeding of IEEE International Conference on Multimedia, pp. 1349-1352, 2006.

[5] Wenjun Zeng1 and Shawmin Lei, "Efficient Frequency Domain Selective Scrambling Of Digital Video", IEEE Transactions on Multimedia, Vol. 5, No. 1, pp. 118-129, 2003.

[6] C. Raju and G.V.R. Sagar, "Scrambling For Privacy Protection and Its Validation in Video Surveillance Systems", International Journal of Engineering Science and Advanced Technology, Vol. 2, No. 3, pp. 712-721, 2012.

[7] Rajat Goel, Ripu R Sinha and O.P. Rishi, "Novel Data Encryption Algorithm", International Journal of Computer Science, Vol. 8. No. 4, pp. 561-565, 2011.

[8] Frederic Dufaux, and Touradj Ebrahimi, "Scrambling for Privacy Protection in Video Surveillance Systems", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 18, No. 8, pp. 1168-1174, 2008.

[9] Isarin Promyarut, Nikom Suvonvorn and Somchai Limsiroratana, "Video Scrambling for Privacy Protection in Surveillance System", In Proceedings of International Conference on Circuits, System and Simulation, Vol. 7, pp. 177-182, 2011.

[10] Jinhaeng Ahn, Hiuk Jae Shim, Byeungwoo Jeon, and Inchoon Choi, "Digital Video Scrambling Method Using Intra Prediction Mode", Springer Lecture Notes on Computer Science, pp. 386-393, 2004.

[11] Nithin Thomas, DavidRedmill and DavidBull, "Secure transcoder for Single Layer Video Data", Signal Processing: Image Communication, Vol. 25, No. 3, pp. 196–207, 2010.

[12] Rogelio Hasimoto-Beltr_an, Shahab Baqai, Ashfaq Khokhar, "Transform Domain inter-block Interleaving Schemes for Robust Image and Video Transmission in ATM Networks", Journal of Visual Communication and Image Representation, Vol. 15, No. 4, pp. 522–547, 2004.