A Technical Survey based on Secure Video Transmission Techniques

Ronak Dak
Dept. of CSE
CTAE,MPUAT, Udaipur,

Dharm Singh
Dept. of CSE
CATE,MPUAT, Udaipur,

Naveen Choudhary
Dept. of CSE
CTAE,MPUAT, Udaipur,

ABSTRACT
With the fast expansion of a variety of multimedia technologies, further and more multimedia statistics are produced and transmitted in the fields like military, medical and for further commercial field which may have some susceptible information that is not to be supposed to be seen or accessed by or may only be shown partially to the common users. Therefore, security and privacy has turn out to be significant phase. Over the last few years numerous encryption algorithms are introduced to secure and protect the video during transmission. Along with that many efficient multimedia encryption schemes are introduced and real world is using those techniques. In this paper, various techniques are observed described showing encryption methods and video transmission techniques have been studied.

General Terms
Pattern Recognition, SCAN Based Patterns, Security, Algorithms et. al.

Keywords
SCAN, DES, Encryption, Entropy NPCR, UACI

1. INTRODUCTION
The significance of securing information has attained the highest levels in recent years due to digital intimidation, intrusion of people's privacy, and the need of communicating exclusive of interference and hacker attacks. In addition, the amalgamation of digital TV with digital video, which is now a reality, and the significant progress in digital libraries make the digital multimedia video on demand the next visible step. It's obvious that multimedia video on demand needs a method capable of offering a good compression ratio, a secure encryption scheme, and a robust hiding scheme for audio, text, and data transmission.

Video Encryption is helpful for preventing eavesdropping (unwanted viewing) of transmitted video, to protect the private videos that are exchanged over the wireless networks and in securing videos for services like video on demand (VOD), Video conferencing and learning. There are a number of algorithms which provide methods to encrypt parts of video frames to make them unrecognizable or secured. But, these all encryption algorithm focuses on complete video data which involves much computation overheads and resource requirements.

2. LITERATURE SURVEY FOR VIDEO ENCRYPTION
With the popularity of wireless networks many researchers have tried to overcome the challenges faced in securing the video data in the real life implementation of wireless technologies. Apart from other issues a lot of work had been contributed to improve the security of videos over wireless networks. In our survey we have studied many such security algorithms, which are provided in this section.

The proposed image encryption [1] is done by replacing the pixel values and permutated pixels values. SCAN method is used to generate scan patterns. In their encryption process, they are using frame differences to encrypt the video. Various frames are encrypted using several keys and encrypted images are generated. Various scan patterns are shown in figure-1.

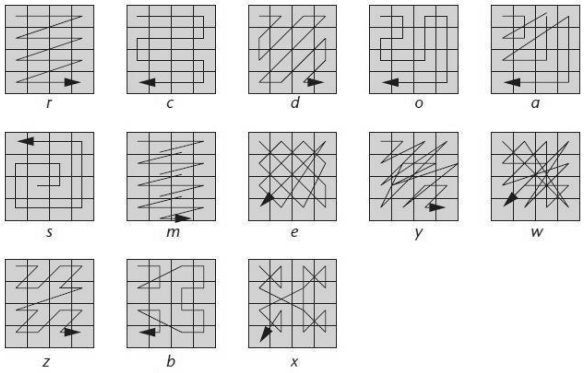

Fig 1: Various scan patterns

The authors of [2] have proposed a encryption method based on SCAN patterns. They have used different SCAN patterns in the single image making it secure enough to be visible. The whole simulation is done on the 256x256 Lena and air fighter images. Several keys are responsible for the pixel rearrangements. These all are simulated on MATLAB 7.1. The lena image and its encryption is shown in figure below:

Fig 2: The lena image and its encryption

In the paper [3], the author says that the algorithm scrambles the position of color image and sets one-to-one relationship between the image matrix and chaotic sequence. Then the pixel value of the scrambled color image is shuffled. The simulation parameters includes histogram, run-time, Correlation between adjacent pixels. High security, confidentiality and efficiency is observed by results and analysis.

The improvement over previous papers can be seen in [4]. This paper researches on a combination of image encryption algorithm, the chaotic encryption and DES encryption. The improved encryption tells about the Logistic chaos sequencer to generate the pseudo-random sequence, furthermore, and then it does double time encryptions along with improvement DES. Basically, the improvement includes reduce in time of DES iterations, expansion of DES E-Box and expansion of key space. Analysis shows that it has high security and speed.

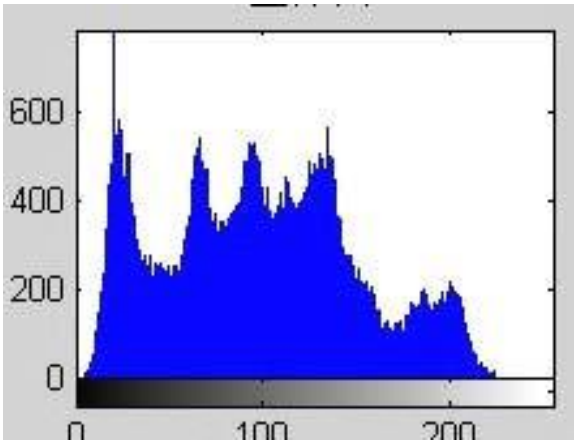

Fig 3: the Histogram Curve of original image

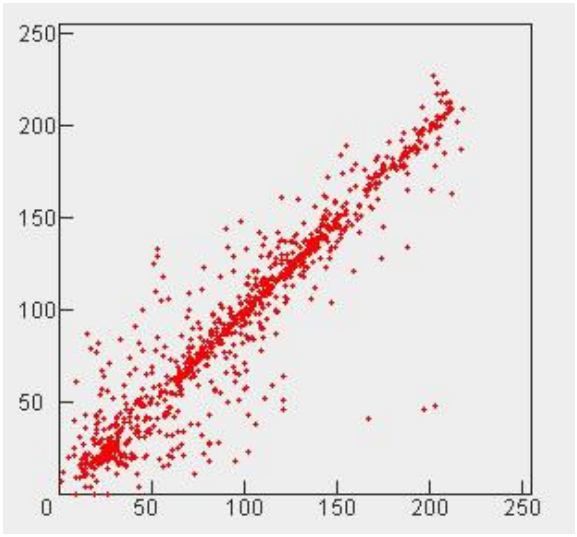

Fig 4: Correlation statistics of original image

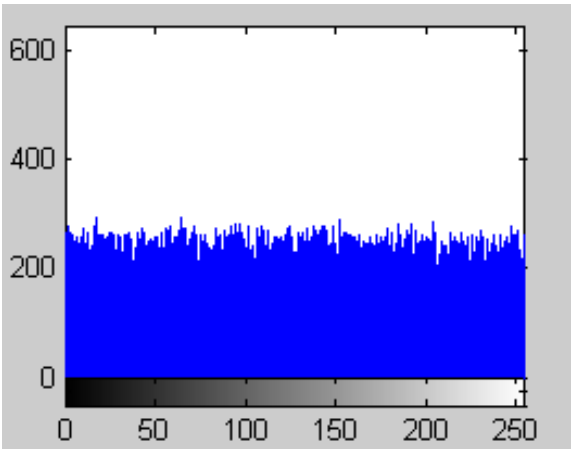

Fig 5: the Histogram Curve of encrypted image

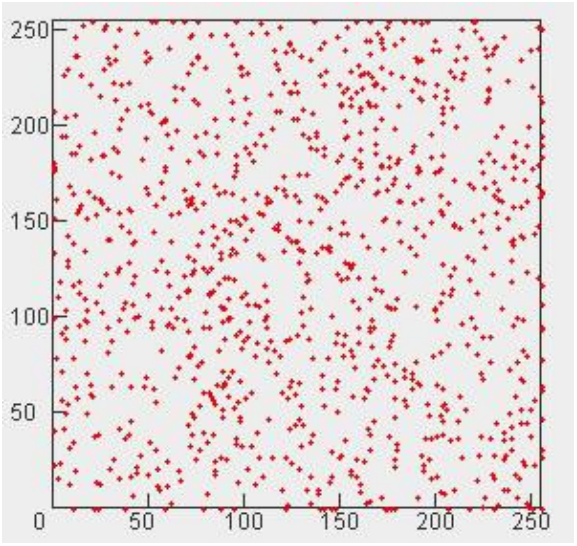

Fig 6: Correlation statistics of encrypted image

Figure 3 and Figure 4 shows the Histogram Curve and Correlation statistics of original image. And Figure 5 and Figure 6 show the Histogram Curve and Correlation statistics of encrypted image.

In [5], authors proposed an image encryption algorithm based on discrete wavelet transform and chaotic map. The algorithm uses the wavelet decomposition. The encryption and decryption is practically applied over sub band image. Wavelet reconstruction is done, to spread the encrypted fraction all over the entire image. To complete the encryption process a second encryption process is used. Analysis and results show satisfied security, as well as increase in efficiency.

A new image encryption algorithm is proposed in this paper which is based on pixels. They show scrambling the image pixel; Elliptic Curve Cryptography (ECC) [6] is used to encrypt the key parameters. Algorithm has high level security due to a large key space and the time required for hiding and encrypting the interactive image tends to $+\infty$.

SCAN methodology [7] can be used for image encryption hybrid technique and encryption using carrier image creation. Alphanumeric keywords are used to create the carrier image. 4 out of 8-code will be generating a unique value according to the given alphanumeric keys. Again, the scan methodology is applied to acquire encrypted image and original image is combined with newly generated carrier image. Highly distorted encrypted image is generated after addition of original and carrier image. In hybrid technique, the consequential image is found to be additional distorted in hybrid technique.

Discrete chaotic logistic map system is used in [8]. They have analyzed the correlation coefficient, Key space, encryption quality and differential attack in chaotic map. Matlab software is used for image encryption and decryption to present Numerical simulations and graphic results.

Codewords based encryption algorithm [9] was proposed for videos. They are first of all shuffling the video frames along with the audio. After that they have used AES to encrypt the sensitive video codewords. Video shredding, shuffling, video stitching and AES encryption computation time is calculated along with other simulation parameters using JAVA, VirtualDUB, PhotoLapse etc for simulation.

In [10] it is described that a plaintext related image encryption method based on chaos and permutation-diffusion architecture [G. Zhang, Q. Liu, Opt. Commun. 284 (2011) 2775-2780]. Then this paper was challenged by Wang et al. that Zhang's scheme cannot resist chosen plaintext attacks [X. Wang, G. He, Opt. Commun. 284 (2011) 5804-5807]. Then, Eslami et al suggested an improvement over Zhang's method with slower encryption speed [Z. Eslami, A. Bakhshandeh, Opt. Commun. 286 (2013) 51-55].

The above was the history of the work. This paper gives another improvement over Eslami's scheme using a lookup table to enhance the speed of encryption algorithm without loss of security. The simulation is carried out on MATLAB and security analysis parameters such as Key Space, Entropy, NPCR, UACI, correlation coefficients are observed.

Table-1

	One Cycle (%)		Two Cycle(%)	
	NPCR	UACI	NPCR	UACI
Zhang et al	0.1181	0.0400	3.0127	1.0116
Eslami et al	99.6083	33.4621	99.6084	33.4610
Proposed	99.6088	33.4692	99.6072	33.4599

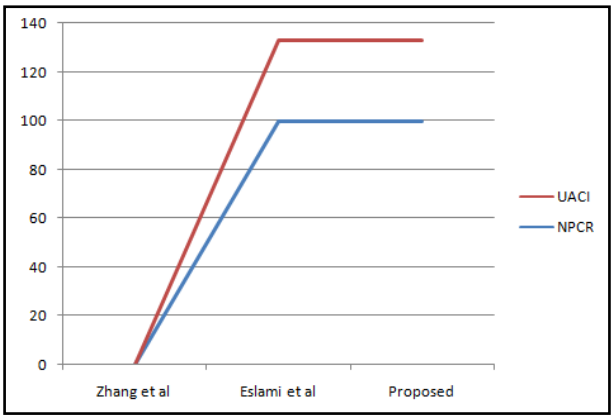

Fig 7: One Cycle

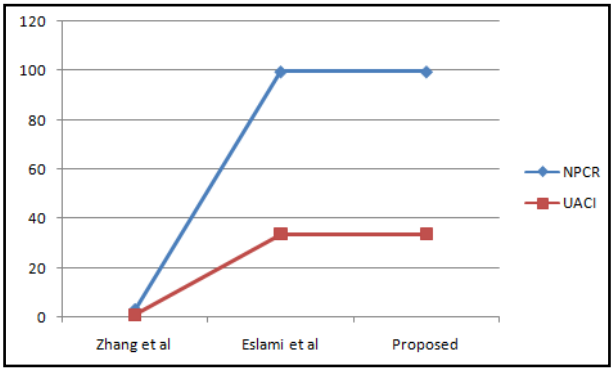

Fig 8: Two Cycle

Decrypted image can be obtained by applying reverse process.

A new thought can be seen in the paper [11]. The proposed method treats the video as a sequence of ordered frames running in a sequence. The algorithm first breaks the video sequence into order of frames by first distributing frames into n frame-sequences and then by internally scrambling these frame sequences using proper keys. These scrambled frame sequences prevent important information like the order of events and can be routed through different network paths for secure video transmission over network. To encrypt the frame sequences, the scheme is suggested to be applied only on videos requiring low security such as long duration entertainment videos. The scheme is extremely cost efficient as the contents of frames are not altered. The scheme is scalable in terms of the number of frame-sequences are formed.

A basic low-cost and zero overhead frame distribution schemes are proposed, which exploits the fact that the video is useful only if its frames are in perfect order. The scale of this distribution is controlled by the factor n. For a video of 1 hour duration and 30 frames per second the brute force space only for step 1 will be equal to 2^{108000}, hence it is sufficient to cause the cost of breaking the algorithm higher than to purchase the key.

3. LITERATURE SURVEY FOR VIDEO TRANSMISSION

A realistic simulation tool-set [12] which integrates EvalVid and NS-2. To support evaluating video transmission over wireless network, they enhanced new interfaces about video transmission and wireless transmission. With the enhancement, the tool-set provides both network related and video-related researchers easily to evaluate video delivered quality of their designs in a simulated environment.

In [13] an algorithm is proposed to enhance system goodput through dynamic optimal fragmentation, in which a sender estimates the SNR of a receiver adaptively and opt a fragmentation threshold to form random sized packets into most favorable length packets. According to wireless channel distinctiveness and lack of QoS hold up, the essential IEEE 802.11 DCF based channel use procedure is merely enough to transport non-real time traffic. The delivery should be amplified by suitable mechanisms to better think about dissimilar QoS necessities and eventually regulate the medium access parameters to the video information content distinctiveness. There is a need to consider prioritized video packet transmission over an error-prone channel to provide more opportunity to transmit higher priority video compared to lower priority to achieve good quality. There are many papers in literature which have considered video prioritization for improving quality.

The robust cross layer architecture [14] is proposed which uses the error resiliency features of H.264 and IEEE 802.11e QoS-based MAC protocol potential to demonstrate the performance of video. The authors of this paper demonstrate that the performance of H.264 video applications can be improved over wireless LANs through a cross layer design, which optimizes the encoded H.264 video slices. They proposed the mechanisms for fragmentation and aggregation of H.264 NALUs (Network Abstraction Layer Units) in order to enhance the quality of decoded video. They showed the video quality can be increased by performing fragmentation in application layer than compared to doing that in MAC layer. They did not consider priorities of video slices and also combining fragmentation at both of these layers.

In [15], the efficiency of video transmissions schemes over 802.11n wireless networks is studied. The focus is centered on the new features introduced at the MAC layer of IEEE 802.11n such as frame aggregation; multiple input multiple outputs (MIMO). In addition, the H.264/AVC video coding standard is exploited to maximize the overall coding efficiency in such wireless network scenario. This study will show that careful parameterization at the MAC and application layers can provide an improve quality of service for many video streaming applications when deployed over an 802.11n network.

4. DISCUSSION

Various video encryption techniques were studied using image encryption methods along with the SCAN based encryption techniques for images. And, it can be evaluated that light weight algorithms also provide good security with less overhead. Then literature about video transmission was thoroughly perceived. Video transmission techniques and tools observed over wireless networks such as 802.11n.

5. REFERENCES

[1] Nikolaos Bourbakis, Apostolos Dollas *"SCAN-Based Compression–Encryption–Hiding for Video on Demand"* 2003 IEEE Published by the IEEE Computer Society

[2] Chao-Shen Chen, and Rong-Jian Chen *"Image Encryption and Decryption Using SCAN Methodology"* Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) 2006 IEEE

[3] Meng Jian-liang Pang Hui-jing Gao Wan-qing "*New color image encryption algorithm based on chaotic sequences ranking"* 2008 IEEE

[4] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping, DAI Wei-di "*Digital Image Encryption Algorithm Based on Chaos and Improved DES"* Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics

[5] M.T. Rodríguez-Sahagún, J.B. Mercado-Sánchez, D. López-Mancilla, R. Jaimes-eátegui, J.H. García-López "*Image Encryption Based on Logistic Chaotic Map for Secure Communications"* 2010 IEEE

[6] Zhu Yu Zhou Zhe Yang Haibing Pan Wenjie Zhang Yunpeng* "*A Chaos-Based Image Encryption Algorithm Using Wavelet Transform"* 2010 IEEE

[7] Guiliang Zhu \ Weiping Wang \ Xiaoqiang Zhang 2, Mengmeng Wang! *"Digital Image Encryption Algorithm Based on Pixels"*2010 IEEE.

[8] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More *"Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study"* International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, March 2013

[9] Yong Zhang, "Encryption Speed Improvement on -An Improvement over An Image Encryption Method Based on Total Shuffling" 2013 IEEE

[10] Jitendra Rajpurohit1, Dr. Ajay Khunteta2 "*A Scalable Frame Scrambling Algorithm for Video Encryption"* Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013)

[11] Panduranga H.T, Naveen Kumar S.K "*Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images"* (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 297-300

[12] Chih-Heng Ke, Cheng-Han Lin "*EVALVID - A Novel Realistic Simulation Tool for Video Transmission over Wireless Network*"

[13] Yusun Chang, Chris Lee, B. Kwon, and John A. Copeland "*Dynamic Optimal Fragmentation for Goodput Enhancement in WLANs*"

[14] Adlen Ksentini and Mohamed Naimi "*Toward an Improvement of H.264 Video Transmission over IEEE 802.11e through a Cross-Layer Architecture*".

[15] aGonçalo Barreira "*Impact of the IEEE 802.11n Frame Aggregation Mechanisms on Video Streaming Quality*".