ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

A improved Scheme for Video Compression Coding and secure authentication using H.264/AVC

Dr.S.Audithan
Principal, P.R.Engineering College, Vallam, Thanjavur, India

Abstract

Among the number of applications available in the internet for users today, video sequences has become ubiquitous and play a major role for knowledge transition, tutorials, lectures for other purposes. In such a context, quality degradation in the video content in terms of even minor quantities will evict a user from using the video. Therefore, minimizing the degradation of video quality from one end to another is a major concern of this research work. Moreover, data is hidden inside the split frames of the video and the secret data is understandable only by the legitimate receiver of the video content. The experimental results conducted based on the proposed algorithm for video compression to avoid quality degradation and securely hiding the sensitive data inside the frames prove that the proposed work is better than the previous works in the literature.

KEYWORDS: Video compression, authentication, watermarking, authentication scheme, quality degradation

1. INTRODUCTION

Video application [1-2] has become one of the dominant applications over Internet, promoted by the rapid development of the network technologies, media coding standards, and the recent advances of the social media network. Security issues arise with the popularity of the video

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

applications, in particular in the wireless consumption [3]. Although the advanced video coding standards, such as H.264/AVC, efficiently reduce the amount of data to be transmitted, the coding dependency brings new challenges in designing efficient stream authentication scheme.

Security issues arise with the popularity of the video applications, in particular in the wireless consumption environments [4-5]. In this research work, the major focus is on the issue of authentication of video stream. The term "authentication" refers to several aspects of security, including integrity, source authenticity and non-repudiation. Integrity refers to that the data is not maliciously changed in transmission. Source authenticity refers to that the media content is indeed sent by the claimed sender. [6] proposed a system in which the cross-diamond search algorithm employs two diamond search patterns (a large and small) and a halfway-stop technique. It finds small motion vectors with fewer search points than the DS algorithm while maintaining similar or even better search quality. The efficient Three Step Search (E3SS) algorithm requires less computation and performs better in terms of PSNR. Modified objected block-base vector search algorithm (MOBS) fully utilizes the correlations existing in motion vectors to reduce the computations. Fast Objected - Base Efficient (FOBE) Three Step Search algorithm combines E3SS and MOBS. By combining these two existing algorithms CDS and MOBS, a new algorithm is proposed with reduced computational complexity without degradation in quality.

In this modern day computer world driven by Facebook, twitter, and other social platforms, the graph authentication based techniques [7] can be used for building the authentication schemes for providing security to the transmitted video by the sender of a video

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

content. The transmission can be carried out in terms of packets of equal or varying lengths. The digital signature thus produced based on this kind of authentication seems to provide a better solution during disputes between a sender and receiver of a video being sent over a lossy channel. Not only the authentication becomes difficult for the sender and receiver, due to inherent problems in the lossy channels, the quality of data gets deteriorated thus leading the problem of video loss and thus spoil the nature of data security [15-17]. For providing security to data, hashing can be used but if excessive hashing may lead to huge overheads for the transmitted data and the two parties for proper data retrieval and verification procedures.

2. LITERATURE SURVEY

This source model consists of rate-quantization, distortion-quantization (D-Q), and distortion-rate (D-R) models [8]. In this part, we first rigorously confirm the accuracy of the proposed source model by comparing the calculated results with the coding data of JM 16.0. Efficient parameter estimation strategies are then developed to better employ this source model in our two-pass rate control method for H.264 variable bit rate coding. Based on our D-Q and D-R models, the proposed method is of high stability, low complexity and is easy to implement.

The encoder and decoder structures of semi-fragile schemes are derived and implemented using nested lattice codes to minimize these two types of errors [9-10]. We then extend the framework to allow the legitimate and illegitimate distortions to be modeled as random noise. In addition, we investigate semi-fragile signature generation methods such that the signature is invariant to watermark embedding and legitimate distortion. A new approach, called MSB

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

signature generation, is proposed which is shown to be more secure than the traditional dual subspace approach. Simulations of semi-fragile systems on real images are provided to demonstrate the effectiveness of nested lattice codes in achieving design objectives.

TESLA, short for Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, strong loss robustness, high scalability, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, short for Efficient Multi-chained Stream Signature, provides non-repudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification.

With the awareness of image content, we formulate an optimization framework, which is able to build an authentication graph yielding the best visual quality at the receiver, given a specific authentication overhead and network condition. Experimental results demonstrate that the proposed scheme achieved our design goals in that the R-D curve of an authenticated image is very close to its original one where no authentication is applied.

There are a number of relevant examples [11-13]which can be cited for graph based authentication schemes being not able to provide enough security to the video contents transmitted by the sender of a sensitive video content. Especially in the H.264 based source encoding technique [14], there is an inherent need for providing and satisfying two ever thirsty parameters such as low authentication and verification probabilities. If one the parameter is increased, the other decreases automatically. These two parameters are inversely proportional to one another and thus, affecting one can lead to the change in another parameter. But, if there is a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

real necessity to provide enhanced authentication to the video content from one party to another party, the transmission line and receiver sides need to incur more overheads for proposer video extraction and secret data.

Based on the drawbacks in the existing works, this research work consists of the following objectives.

(i) To recognize the importance of the source coding and channel coding context in the design of optimized end-to-end quality authentication schemes.

(ii) To securely transfer the secret image file as well as data hidden in the frames of the video to the receiver side.

3. PROPOSED SYSTEM ARCHITECTURE

The architecture of the proposed system is clearly portrayed in figure 1. A novel layered authentication framework called Joint Media Error and Authenticity Protection (JMEAP) in order to apply it on JPEG- 2000 images has been proposed in this research work. The layered schemes jointly consider the Authentication and transmission over loss networks, therefore both high verification probability and low authentication. The proposed architecture consists of four modules. One of the modules is for video uploading which uploads the video content. Another module called video preprocessing module does the preprocessing work. Third module is video hiding module which secretly hides the data into selected frames of the video and the fourth module is that of extracting the secret data from the received video sequence.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

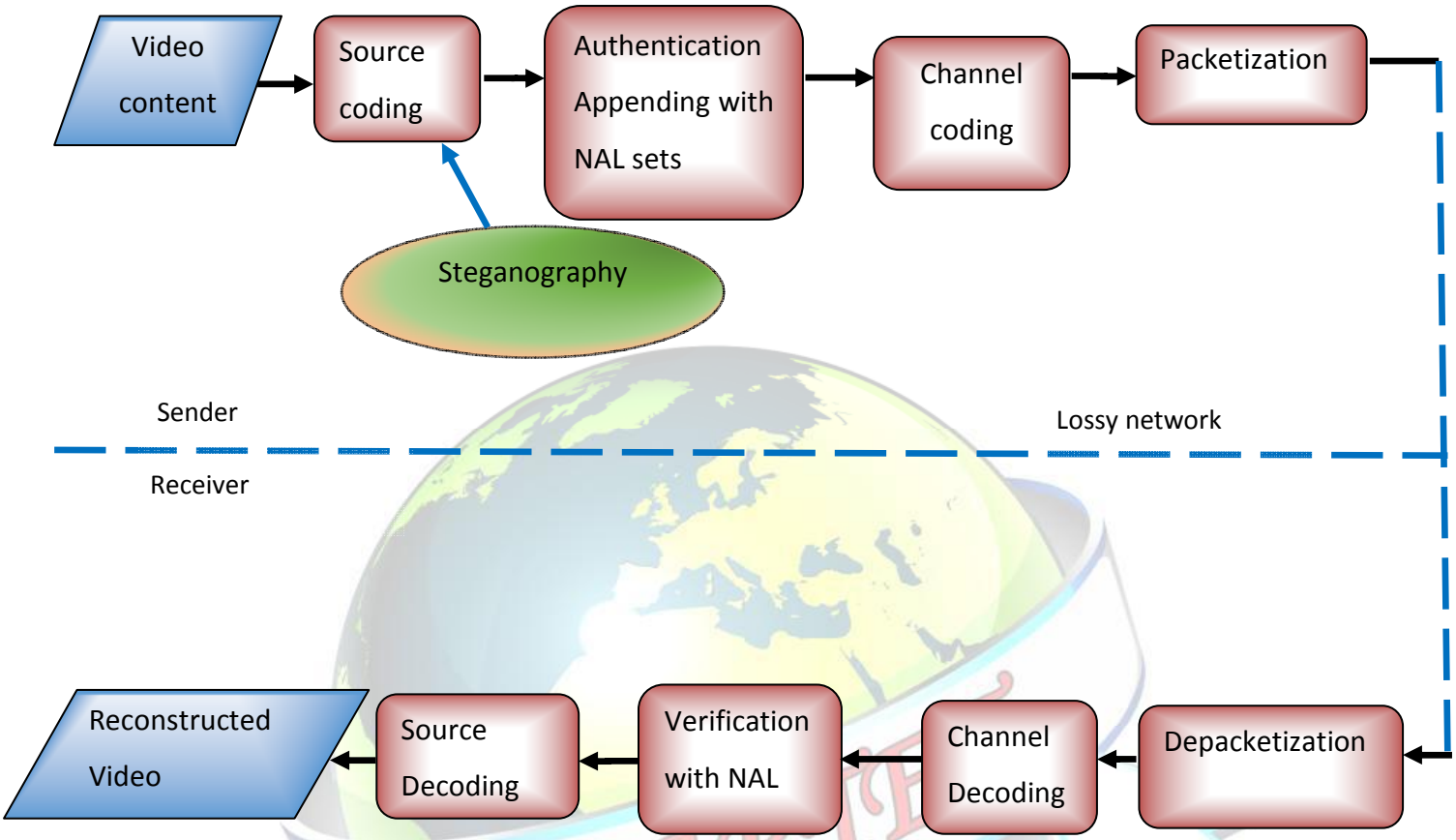

Fig.1 Architecture of the proposed system

The invisible watermarking technique is used to select the frames and the frames in which the data is hidden are converted into video. Subsequently, the video is sent to the receiver side. In the receiver side, the video is decrypted and split into component frames and the user extracts the secret image and data by selecting the specific frames which was watermarked. Ultimately, the video is decoded in an attempt to identify the loss of content.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

4. THE PROPOSED SCHEME

The proposed algorithm for efficient authentication and video compression is described below. It consists of the step by step procedure for splitting the video into its constituent frames, numbering the frames, application of steganography and the watermarking technique for authentication and secure transmission of data by selecting a specific set of frames in the video. Subsequently, the video is encoded using the agreed upon RSA algorithm. The encrypted video is then transferred to the receiver side for decryption and the data and images are very well separated as described in the algorithm.

//INPUT:video, image, secret data

//OUTPUT:video without loss, secret data

1. Upload video

   //video split into frames

2. for i=1 to n frames

   Using steganography and watermarking technique encrypt the message into selected frames.

3. STEGANOGRAPHY

   Convert into grayscale image and hide a secret data

   And it get convert stegano image and apply least significant bit

   Split image into n blocks

   Apply DCT to each block

4. WATERMARKING TECHNIQUE

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

for i=1:m

for j=1:n

$$\mathbf{l_{xw}(i,j) = I_x(i,j) + \alpha I_w(i,j)}$$

else

$$\mathbf{l_{xw}(i,j) = I_x(i,j)}$$

end

end

5. Create the cipher text using the RSA algorithm.
6. Hash the NAL[ ]set.
7. Create video from frames and send it.
8. Receiver decrypts the video along with the hidden data.
9. Video= video+frames[i];

The proposed system is based on the video upload module in which a sender who wants to send a video uploads it so as to embed the secret information into it. In the video preprocessing module, the given video is split such that, the video is output as frames and some of the frames are selected for hiding the data and are also encoded. The data is hidden in the frame with the help of the watermarking technique and this is done in the watermarking module. In the final module, the video received from the sender is split into its constituent frames and the frame which contains the secret is identified and the hidden sensitive data is extracted as well.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

5. IMPLEMENTATION

The proposed system has been implemented in the C#.Net (2.95GHz and above processor, 2GB RAM, 80 GB Hard Disk, Windows 7 Operating system) for a secure transmission of data through video frames.

.NET Framework's Base Class Library provides user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. Programmers produce software by combining their own source code with .NET Framework and other libraries. .NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces an integrated development environment largely for .NET software called Visual Studio.

Fig.3 LOGIN WINDOW

In figure 3, a user logs into the system for secure data transmission through the video sequence. Figure 4 shows the processing of the system during system login. In figure 5, the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

options available to user are clearly depicted. Figure 6 shows a user uploading the file. Figure 3 to Figure 11 show the effective of the algorithm during its implementation.

Fig.4 Main window

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

Fig. 5 USER HOME

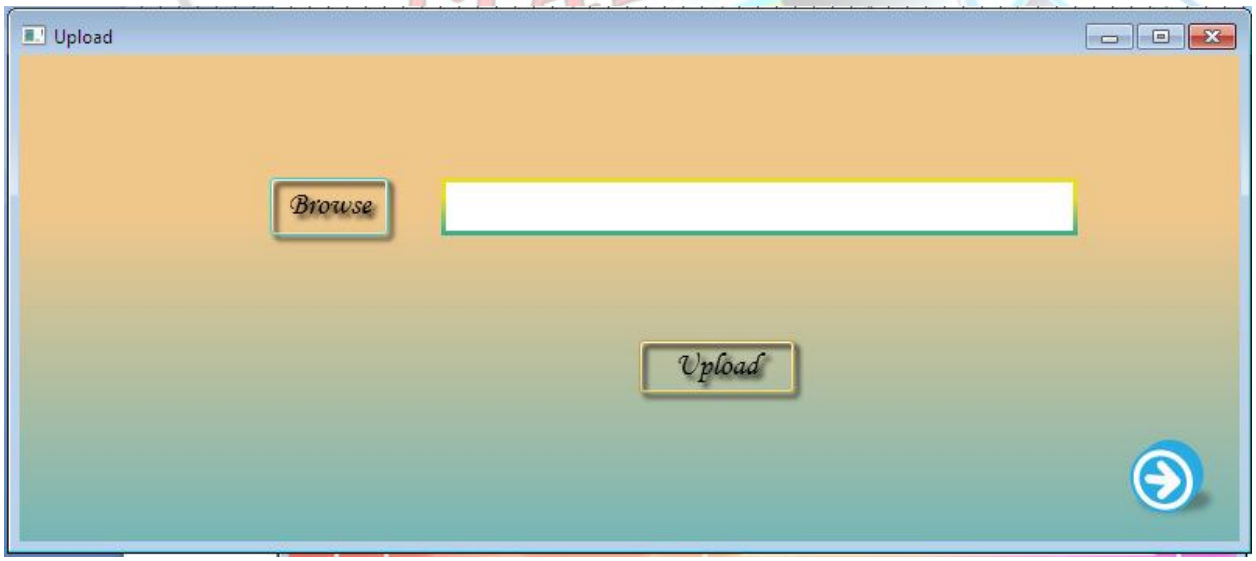

Fig. 6 Video upload

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

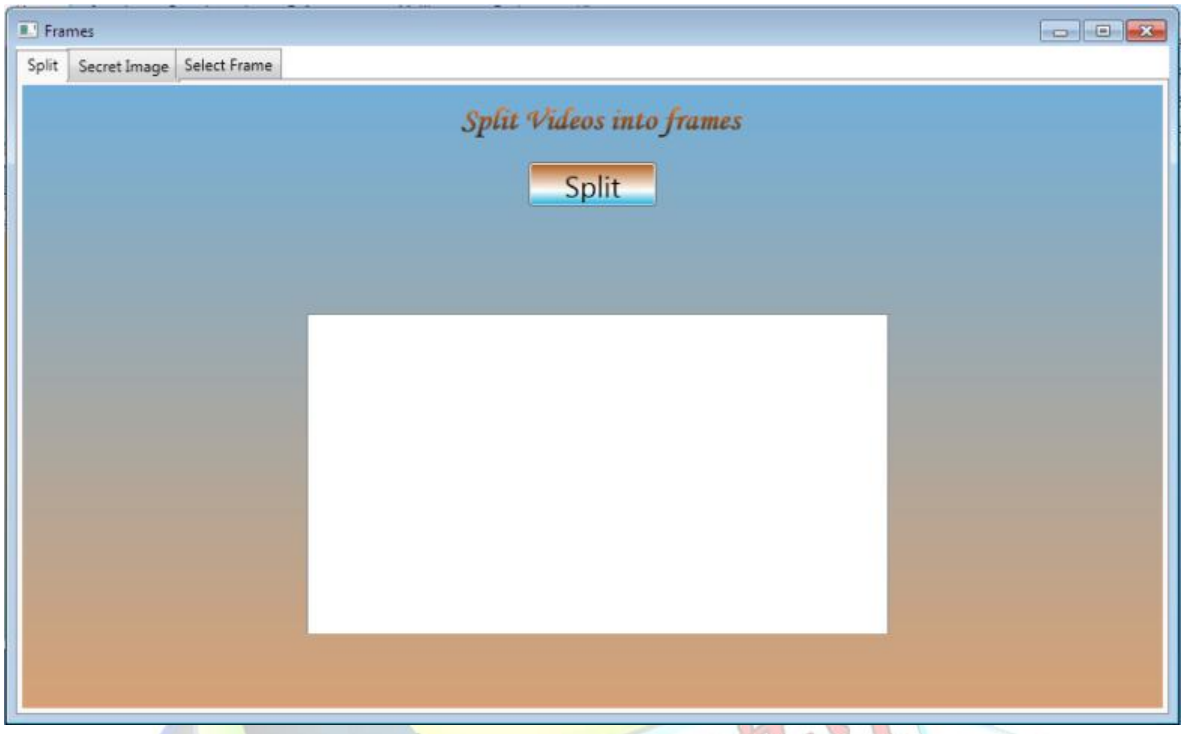

Fig. 7 Frames - Secret Image

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

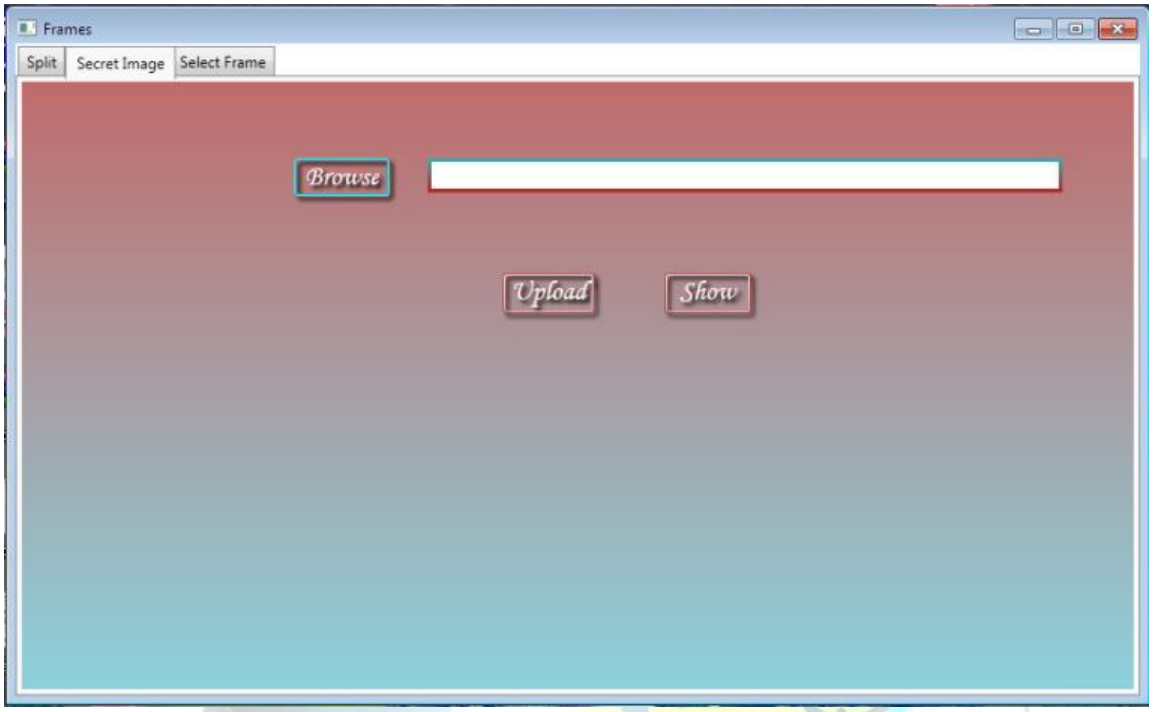

Fig.8 Select Frame

Fig.9 Hide Image-Grayscale Conversion

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

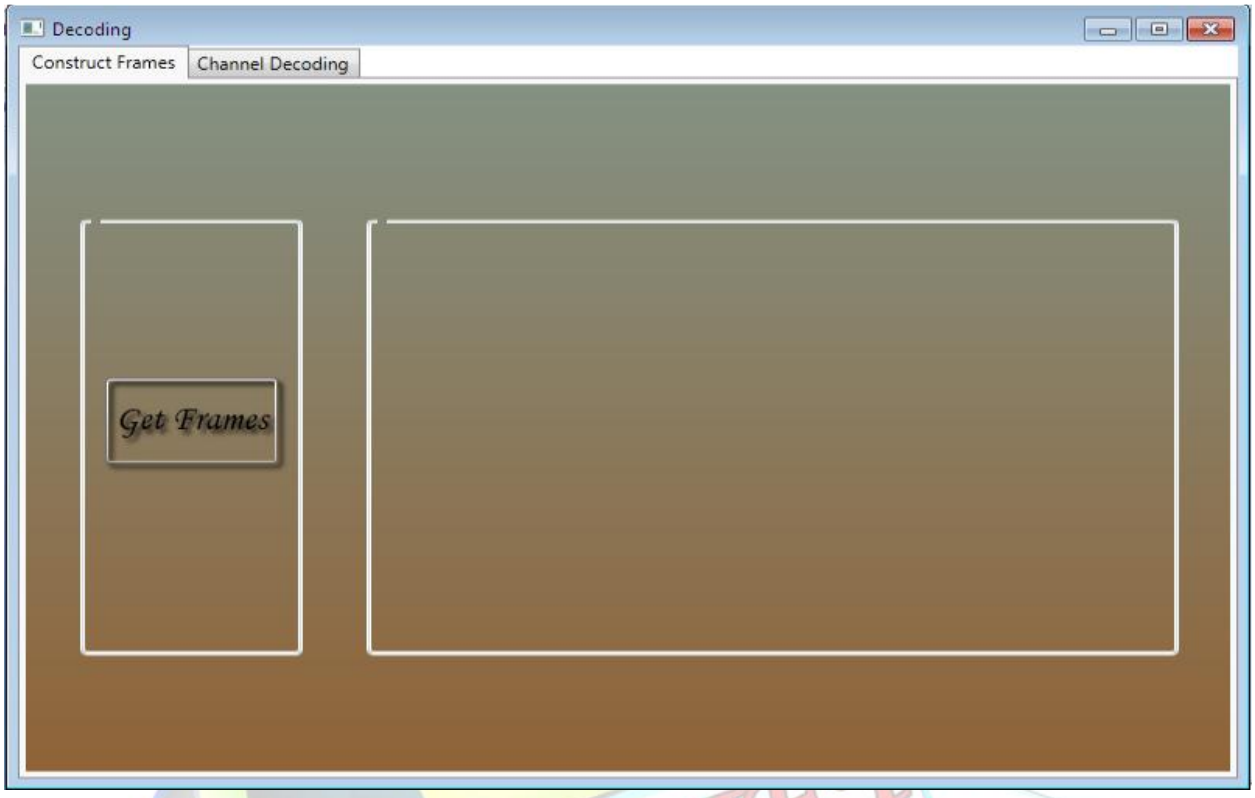

Fig.10 Decoding-Construct Frames

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

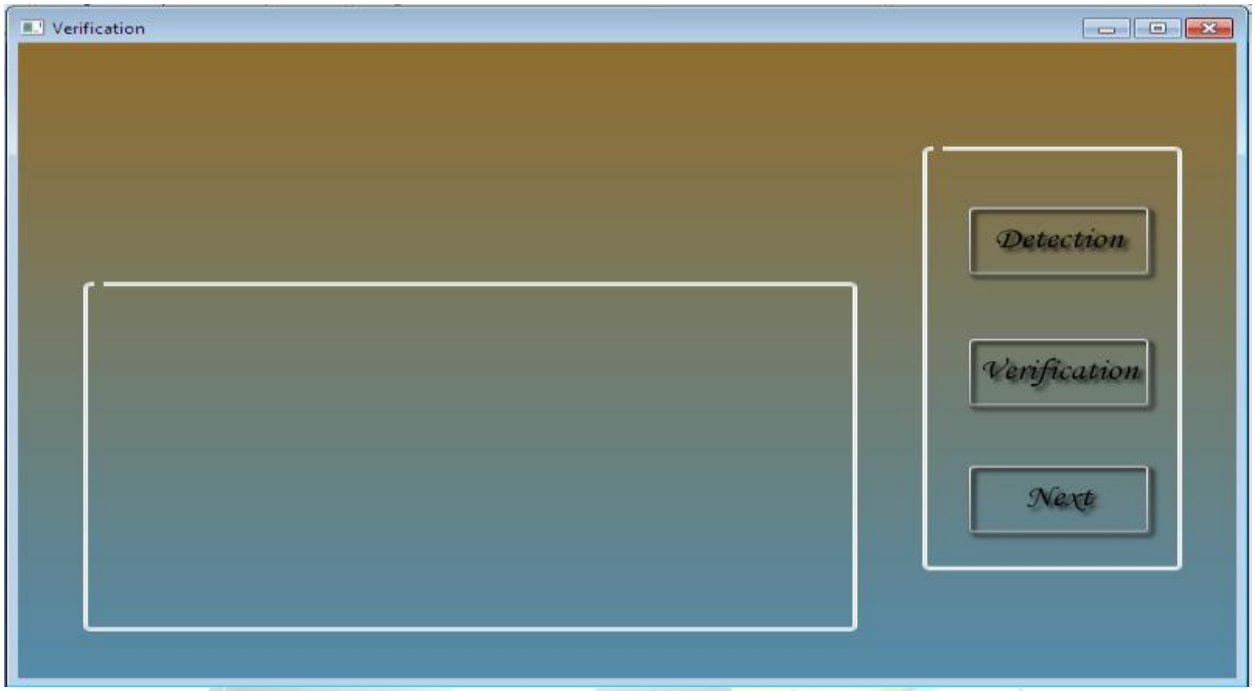

Fig.11 Verification

6. CONCLUSIONS AND FUTURE WORKS

The proposed Scheme is able to achieve 100% effective verification probability while maintaining low authentication overhead, i.e., all media slices recovered from the lossy channel can be decoded and authenticated and show that the authentication overhead is low. The eminent future works of this research work relies on the successful transmission of secure data based on BASE 64 coding technique. Forming the entire system to be a high performance capability and low error transmission can be useful research in this direction. Its applications include the reduction of of transmission and error rate for video streams.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

REFERENCES

[1] Xinglei Zhu, Chang Wen Chen, "A Joint Source-Channel Adaptive Scheme for Wireless H.264/AVC Video Authentication", IEEE Transactions on Information Forensics and Security, Vol. 11, No. 1, pp. 141-153, 2016.

[2] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Proc. IEEE Symposium on Security and Privacy, pp. 56–73, 2000.

[3] Z. Li, Q. B. Sun, and Y. Lian, "Unequal authenticity protection (UAP) for rate-distortion-optimized secure streaming of multimedia over wireless networks", in the Proc. IEEE International Symposium on Circuits and Systems, 2006.

[4] Z. Li, Q. B. Sun, Y. Lian, and Chang Wen Chen. Authenticating multimedia transmitted over wireless networks: A content-aware stream level approach. In Proc. IEEE ICME, 2006.

[5] Z. He and S.K. Mitra, "A unified rate-distortion analysis framework for transform coding. IEEE Transactions on Circuits and Systems for Video Technology", 11(12):1221–1236, 2001.

[6] Christo Ananth, A.Sujitha Nandhini, A.Subha Shree, S.V.Ramyaa, J.Princess, "Fobe Algorithm for Video Processing", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), Vol. 3, Issue 3,March 2014 , pp 7569-7574

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

[7] Z. Li, Q. Sun, Y. Lian, and C. W. Chen, "Joint source-channel authentication resource allocation and unequal authenticity protection for multimedia over wireless networks," IEEE Trans. Multimedia, vol. 9, no. 4, pp. 837–850, Jun 2007.

[8] R. Gennaro and P. Rohatgi, "How to sign digital streams," in Advances in Cryptology, pp. 180–197, 1997.

[9] C.S. Lu and H.-Y. M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," IEEE Trans. Multimedia, vol. 5, no. 2, pp. 161–173, 2003.

[10] Jun Sun, Yizhou Duan, Jiangtao Li, Jiaying Liu, Zongming Guo, "Rate-Distortion Analysis of Dead-Zone Plus Uniform Threshold Scalar Quantization and Its Application—Part I: Fundamental Theory", IEEE Transactions on Image Processing, Vol 22, No.1, pp. 202-214, 2013.

[11] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 43–55, 2006.

[12] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in Proc. IEEE Int. Conf. Image Processing (ICIP), Lausanne, Switzerland, Sep. 1996, pp. 243–246.

[13] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Process., vol. 66, no. 3, pp. 283–301, 1998.

[14] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, "Real-time labeling methods for MPEG compressed video," in Proc. 18th Symp. Inf. Theory Benelux, Veldhoven, The Netherlands, May 1997.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 1, January 2017

[15] T.-Y. Chen, V. Istanda, T.-H. Chen, D.-J. Wang, and Y.-L. Lin, "H.264 video authentication based on semi-fragile watermarking," International Journal ofInnov. Comput., Inf. Control, Vol. 6, no. 3, pp. 1411–1420, 2010.

[16] B. G. Mobasseri and Y. N. Raikar, "Authentication of H.264 streams by direct watermarking of CAVLC blocks," Proc. SPIE, Security, Steganography, Watermarking Multimedia Contents IX, Vol. 6505, no. 1W, pp. 1–5, Feb. 2007.

[17] X. Gong and H.-M. Lu, "Towards fast and robust watermarking scheme for H.264 video," in Proc. IEEE Int. Symp. Multimedia, pp. 649–653, 2008.