AVC Video Codec and Data Hiding

[1]S.Vyshnavi, [2]B.Venkata Kiran, [3]K.Satya Rahul
[1]Student, [2]Student, [3]Assistant Professor
Godavari Institute Of Engineering And Tecnology

Abstract - **Digital video sometimes needs to be to perform and processed in an encrypted format to maintain security and privacy. For the purpose of content notation or tampering detection, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. In addition, it is more efficient without decryption followed by data hiding and re-encryption. In this paper a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed which includes the following three parts, H.264/AVC video encryption, data embedding, and data extraction. By analyzing the property of H.264/AVC codec, the codewords of intraprediction modes, the codewords of residual coefficients are encrypted with stream ciphers. Then a data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content. In order to adapt to different application scenarios data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly preserved even after encryption and data embedding. Experimental results have demonstrated the feasibility and efficiency of the proposed scheme.**

keywords - **H.264,data hiding, hiding keys, encryption, AVC.**

I. INTRODUCTION

H.264 is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. Video compression is an essential technology for applications such as digital television, DVD-video, mobile TV, videoconferencing and internet video streaming. Standardising video compression makes it possible for products from different manufactures to inter-operate. An encoder converts video into a compressed format and a decoder converts compressed video back into an uncompress format.

Recommendation H.264: Advanced video coding is a document published by the international standards bodies ITU-T(International Telecommunication Union) and ISO/IEC (International Organisation for Standardization). It defines a format or syntax for compressed video and a method for decoding this syntax to produce a displayable video sequence. The standard document does not actually specify how to encode (compress) digital video – this is left to the manufacturer of a video encoder – but in practice the encoder is likely to mirror the steps of the decoding process.

II. LITERARY SURVEY

H.264/AVC is latest video coding standard of the ITU-T Video Coding Experts Group and the ISO/IEC Moving Picture Experts Group. The main goals of the H.264/AVC Standardization effort have been enhanced compression Performance and prerequisite of a network- friendly‖ Video representation addressing —conversational‖ (video Telephony) and no conversational‖ (storage, broadcast, or Streaming) applications. H.264/AVC has achieved a Significant improvement in rate-distortion efficiency Comparative to existing standards.

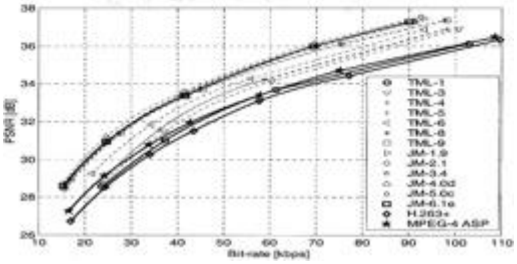


Fig. 1. EVOLUTION OF H.264/AVC SINCE AUGUST 1999 UNTIL MARCH 2003 .

III. APPROACH

SYSTEM ARCHITECTURE

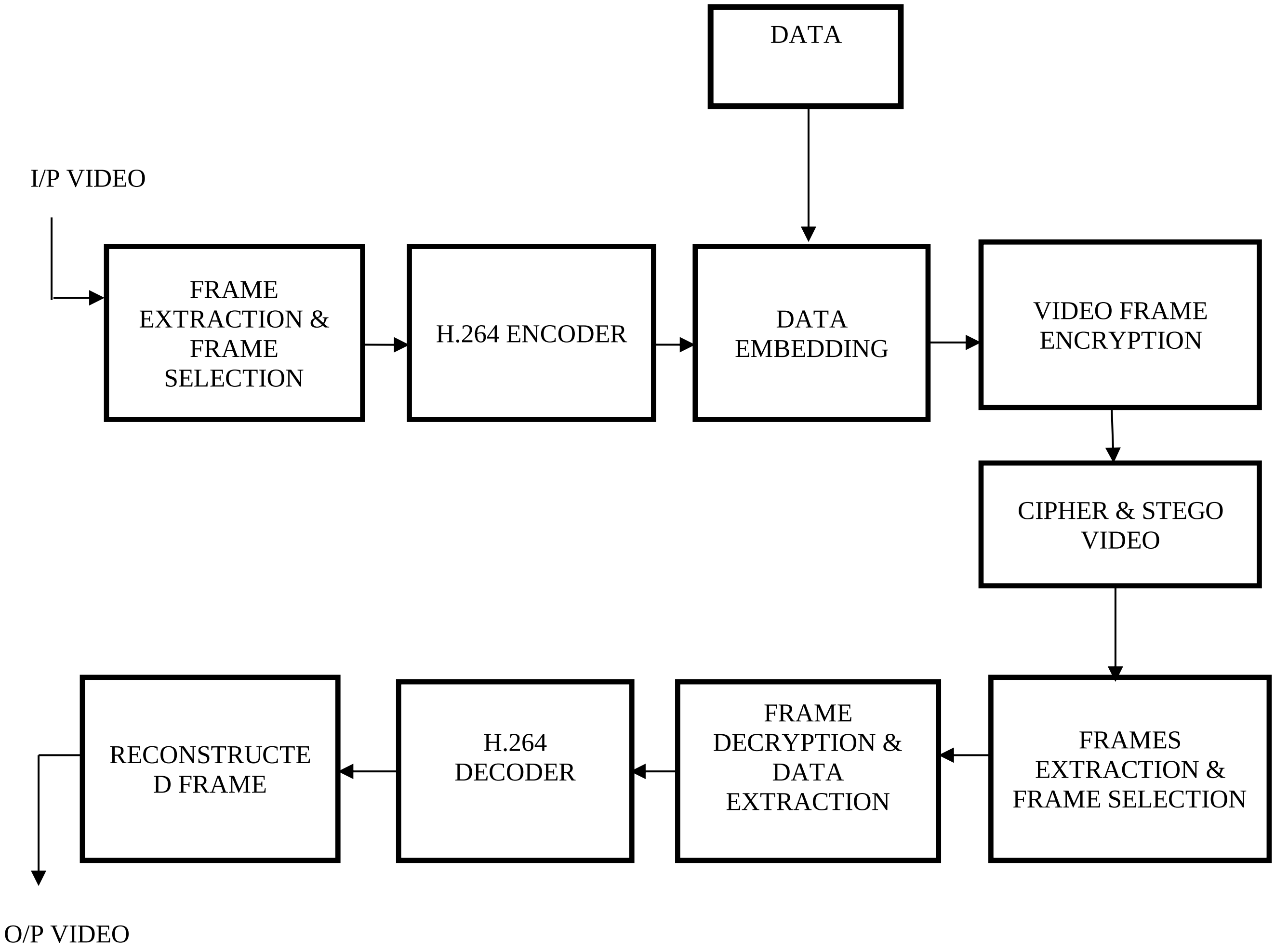


Figure 2 : System Architecture

EDGE PROPERTIES :

The edges extracted from a two-dimensional image of a three-dimensional scene can be classified as either viewpoint dependent or viewpoint independent. A viewpoint independent edge typically reflects inherent properties of the three-dimensional objects, such as surface markings and surface shape. A viewpoint dependent edge may change as the viewpoint changes, and typically reflects the geometry of the scene, such as objects occluding one another.

A typical edge might for instance be the border between a block of red color and a block of yellow. In contrast a line (as can be extracted by a ridge detector) can be a small number of pixels of a different color on an otherwise unchanging background. For a line, there may therefore usually be one edge on each side of the line. LSB substitution technique is proposed for data embedding and extraction

Edge detection includes a variety of mathematical methods that aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed edges. The same problem of finding discontinuities in one-dimensional signals is known as step detection and the problem of finding signal discontinuities over time is known as change detection. Edge detection is a fundamental tool in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extraction.

The purpose of detecting sharp changes in image brightness is to capture important events and changes in properties of the world. It can be shown that under rather general assumptions for an image formation model, discontinuities in image brightness are likely to correspond to:

- discontinuities in depth,
- discontinuities in surface orientation,
- changes in material properties and
- variations in scene illumination.

In the ideal case, the result of applying an edge detector to an image may lead to a set of connected curves that indicate the boundaries of objects, the boundaries of surface markings as well as curves that correspond to discontinuities in surface orientation. Thus, applying an edge detection algorithm to an image may significantly reduce the amount of data to be processed and may therefore filter out information that may be regarded as less relevant, while preserving the important structural properties of an image. If the edge detection step is successful, the subsequent task of interpreting the information contents in the original image may therefore be substantially simplified. However, it is not always possible to obtain such ideal edges from real life images of moderate complexity.

Edges extracted from non-trivial images are often hampered by fragmentation, meaning that the edge curves are not connected, missing edge segments as well as false edges not corresponding to interesting phenomena in the image – thus complicating the subsequent task of interpreting the image data.
Edge detection is one of the fundamental steps in image processing, image analysis, image pattern recognition, and computer vision techniques.

DATA HIDING :

- In this stage, we perform the data hiding.
- In that, secret data will be hided into the compressed frame based on edge based least significant bit method.
- Here, hybrid edge detection model is proposed. The hybrid models are such as Canny and LOG edge detection. Based on the canny and log, edge image was obtained from image.
- Then classify the pixels of the compressed frame into two categories which are non-edge pixels and edge pixels, respectively.
- After that, secret data is embedded in non-edge pixel of compressed frame.

DATA EMBEDDING :

In video coding, intra frame is more important than other (B or P) frames. H.264 is high compression and neighbouring dependence. If errors occur, therefore, any change on intra frame will make error propagation effect on B or P frames. Most of error resilient techniques may solve this problem. However, they sacrificed the video quality for embedding image itself. If the transmission is error-free, the image quality can not be exactly recovered by H.264 in the decoder. To solve this problem, a technique combines error resilience and reversible data embedding is proposed. The proposed resilient algorithm employs a reversible data embedding technique in residual DCT coefficients of intra block.

DATA FLOW

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.
The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.
The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.
The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS :

The Primary goals in the design of the UML are as follows:

- Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modeling language.
- Encourage the growth of OO tools market.
- Support higher level development concepts such as collaborations, frameworks, patterns and components.
- Integrate best practices.

CIPHERTEXT :

Ciphertext or cyphertext is the result of encryption performed on plaintext using an algorithm, called a cipher. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with code text because the latter is a result of a code, not a cipher.

Modern ciphers are more secure than classical ciphers and are designed to withstand a wide range of attacks. An attacker should not be able to find the key used in a modern cipher, even if he knows any amount of plaintext and corresponding ciphertext.

Modern encryption methods can be divided into the following categories:

- Private-key cryptography (symmetric key algorithm): the same key is used for encryption and decryption
- Public-key cryptography (asymmetric key algorithm): two different keys are used for encryption and decryption

In a symmetric key algorithm (e.g., DES and AES), the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm (e.g., RSA), there are two separate keys: a public key is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables only him to perform correct decryption.

Symmetric key ciphers can be divided into block ciphers and stream ciphers. Block ciphers operate on fixed-length groups of bits, called blocks, with an unvarying transformation. Stream ciphers encrypt plaintext digits one at a time on a continuous stream of data and the transformation of successive digits varies during the encryption process.

***USE CASE DIAGRAM* :**

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

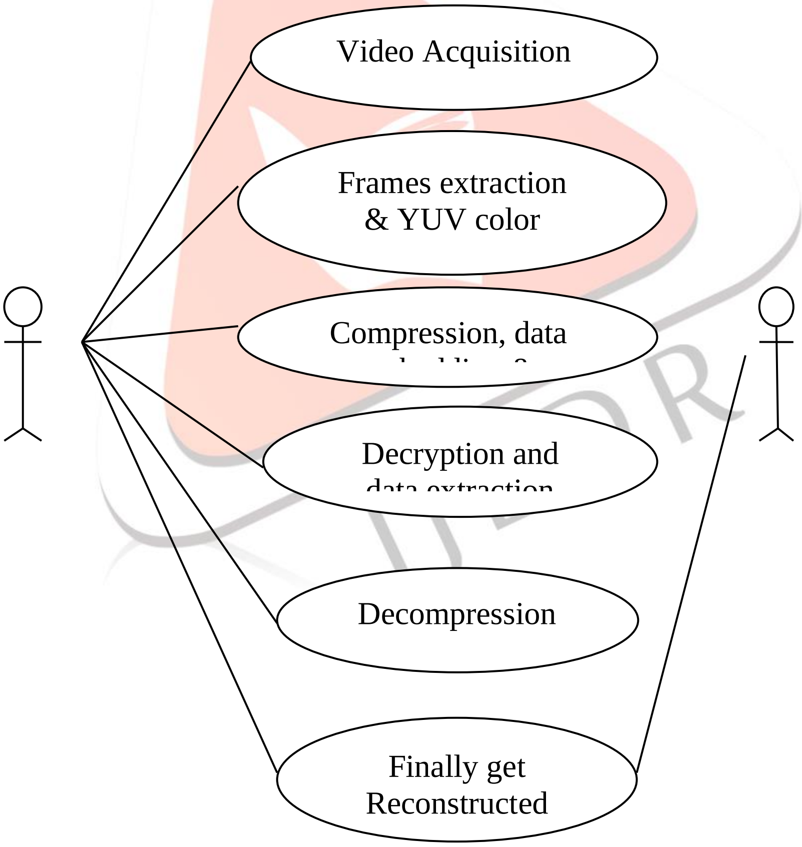


Figure 3 : Use case Diagram

In this paper, an efficient commutative encryption and data hiding scheme based on H.264 codec is presented, which provides reliability control functionalities. Data embedding and video encryption are accomplished during H.264 compression process. The security analysis results demonstrated and proved the proposed scheme can achieve perception security and cryptographic security. Furthermore, experimental results also show that the video distortion caused by data hiding is very low and that the achieved capacity is enough to embed a reliability proof as well as some other data.

Key management is a critical issue in all encryption based security systems, as it cannot be separated from the design of secure multimedia distribution. In most distribution architectures, multimedia content is encrypted with a symmetric key which also needs to be protected in transmission to the receiver. Hence, the storage and security requirements of key management need to be discussed in greater detail in future proposals.

Another feature that may be added to the proposed selective schemes is the selection criteria. Encryption techniques can be chosen dynamically as the content is being distributed and the selection criteria can be changed as needed by the application. Enhancement in compression performance by introduction of new functionalities which also improves security as encryption is combined with compression.

In this paper, an efficient commutative encryption and data hiding scheme based on H.264 codec is presented, which provides reliability control functionalities. Data embedding and video encryption are accomplished during H.264 compression process. The security analysis results demonstrated and proved the proposed scheme can achieve perception security and cryptographic security. Furthermore, experimental results also show that the video distortion caused by data hiding is very low and that the achieved capacity is enough to embed a reliability proof as well as some other data.

Key management is a critical issue in all encryption based security systems, as it cannot be separated from the design of secure multimedia distribution. In most distribution architectures, multimedia content is encrypted with a symmetric key which also needs to be protected in transmission to the receiver. Hence, the storage and security requirements of key management need to be discussed in greater detail in future proposals.

Another feature that may be added to the proposed selective schemes is the selection criteria. Encryption techniques can be chosen dynamically as the content is being distributed and the selection criteria can be changed as needed by the application. Enhancement in compression performance by introduction of new functionalities which also improves security as encryption is combined with compression.

INTRA PREDICTION METHOD (INTRA FRAME CODING) :

Intra-frame coding is used in video coding (compression). It is part of an intra-frame codec like ProRes: a group of pictures codec without inter frames.

Intra-frame prediction exploits spatial redundancy, i.e. correlation among pixels within one frame, by calculating prediction values through extrapolation from already coded pixels for effective delta coding. It is one of the two classes of predictive coding methods in video coding. Its counterpart is inter-frame prediction which exploits temporal redundancy. Temporally independently coded so-called intra frames use only intra coding. The temporally coded predicted frames (e.g. MPEG's P- and B-frames) may use intra- as well as inter-frame prediction.

Usually only few of the spatially closest known samples are used for the extrapolation. Formats that operate sample by sample like Portable Network Graphics (PNG) can usually use one of four adjacent pixels (above, above left, above right, left) or some function of them like e.g. their average. Block-based (frequency transform) formats prefill whole blocks with prediction values extrapolated from usually one or two straight lines of pixels that run along their top and left borders.

The term intra-frame coding refers to the fact that the various lossless and lossy compression techniques are performed relative to information that is contained only within the current frame, and not relative to any other frame in the video sequence. In other words, no temporal processing is performed outside of the current picture or frame. Non-intra coding techniques are extensions to these basics. It turns out that this block diagram is very similar to that of a JPEG still image video encoder, with only slight implementation detail differences.

INTER PREDICTION METHOD (INTER FRAME CODING) :

An inter coded frame is divided into blocks known as macroblocks. After that, instead of directly encoding the raw pixel values for each block, the encoder will try to find a block similar to the one it is encoding on a previously encoded frame, referred to as a reference frame. This process is done by a block matching algorithm. If the encoder succeeds on its search, the block could be encoded by a vector, known as motion vector, which points to the position of the matching block at the reference frame. The process of motion vector determination is called motion estimation.

In most cases the encoder will succeed, but the block found is likely not an exact match to the block it is encoding. This is why the encoder will compute the differences between them. Those residual values are known as the prediction error and need to be transformed and sent to the decoder.

To sum up, if the encoder succeeds in finding a matching block on a reference frame, it will obtain a motion vector pointing to the matched block and a prediction error. Using both elements, the decoder will be able to recover the raw pixels of the block.

Inter prediction creates a prediction model from one or more previously encoded video frames. The model is formed by shifting samples in the reference frame(s) (motion compensated prediction). The AVC CODEC uses block-based motion compensation, the same principle adopted by every major coding standard since H.261. Important differences from earlier standards include the support for a range of block sizes (down to 4x4) and fine sub-pixel motion vectors (1/4 pixel in the luma component).

DIFFERENCES BETWEEN H.263 AND H.264:

H.263	*H.264*
1. pixel accuracy is 1/2	1. Pixel accuracy is 1/4
2. Reference picture required is 1	2. Reference picture required is 16
3. Complexity is medium	3. Complexity is high
4. Transform into 8x8 DCT form	4. Transforms into 4x4 integral form

IV. RESULTS

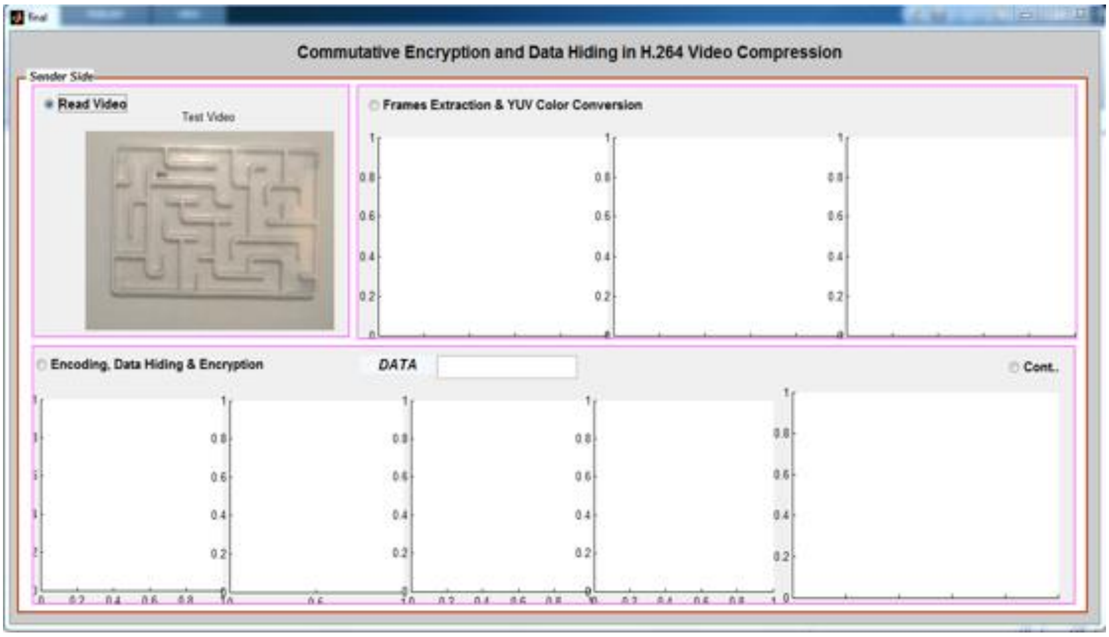
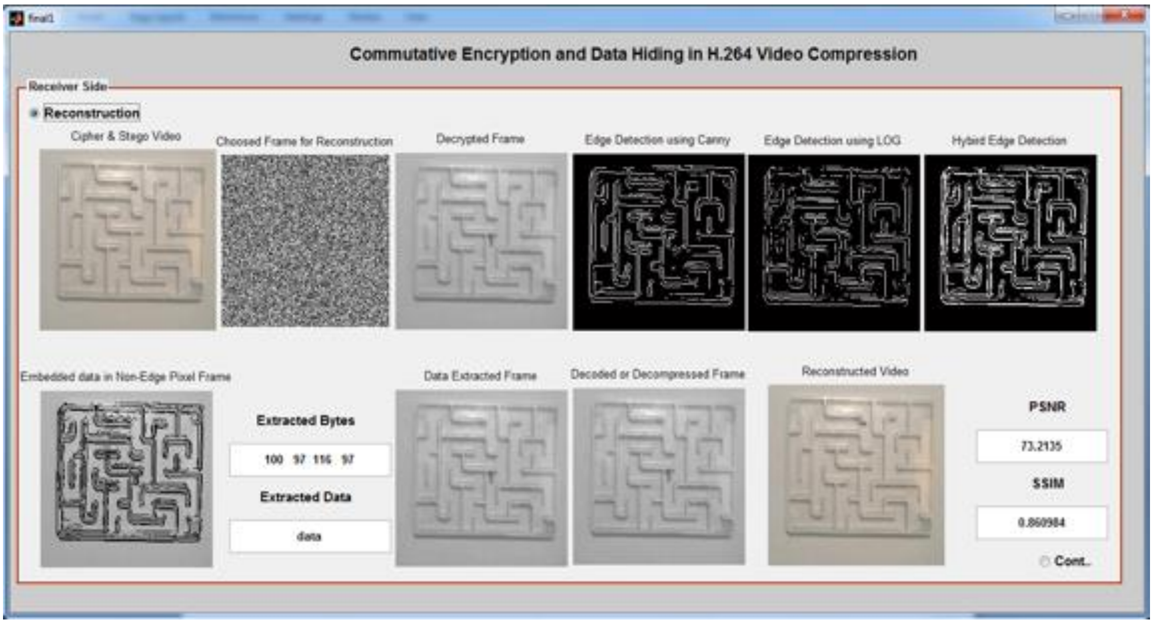

final
Commutative Encryption and Data Hiding in H.264 Video Compression
Sender Side
● Read Video
Test Video
○ Frames Extraction & YUV Color Conversion
○ Encoding, Data Hiding & Encryption
DATA
○ Cont.
0.2
0.4
0.6
0.8
1

Figure 4 : Reading a video from the system


final1
Commutative Encryption and Data Hiding in H.264 Video Compression
Receiver Side
● Reconstruction
Cipher & Stego Video
Choosed Frame for Reconstruction
Decrypted Frame
Edge Detection using Canny
Edge Detection using LOG
Hybrid Edge Detection
Embedded data in Non-Edge Pixel Frame
Data Extracted Frame
Decoded or Decompressed Frame
Reconstructed Video
○ Cont.

Extracted Bytes: 100 97 116 97

Extracted Data: data

PSNR: 73.2135

SSIM: 0.860984

Figure 5 : Reconstruction video

V. CONCLUSION

In this paper, the PSNR of the decoded video sequence always exhibit a similar behavior; i.e. .the quality steadily decreases with the increment of the quantization factor. The results obtained in these experiments points out the high correlation between the AQI and the human visual system for H.264 video coded sequences, in contrast with the PSNR, as a reliable way to measure the perceptual quality of images. This fact opens the possibility of incorporating self-regulated compression parameters depending on the perceptual quality.

I. References

[1] B. Boyadjis, C. Bergeron, B. Pesquet-Popescu, and F. Dufaux, ``Extended selective encryption of H. 264/AVC (CABAC)- and HEVC-encoded video streams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 4, pp. 892_906, Apr. 2017.

[2] A. I. Sallam, O. S. Faragallah, and E.-S. M. El-Rabaie, ``HEVC selective encryption using RC6 block cipher technique," *IEEE Trans. Multimedia*, vol. 20, no. 7, pp. 1636_1644, Jul. 2018.

[3] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, ``Arobust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," *IEEE Access*, vol. 5, pp. 5354_5365, Apr. 2017.

[4] D. Xu, R. Wang, and J. Wang, ``Prediction mode modulated data-hiding algorithm for H.264/AVC," *J. Real-Time Image Process.*, vol. 7, no. 4, pp. 205_214, Dec. 2012.

[5] H. A. Aly, ``Data hiding in motion vectors of compressed video based on their associated prediction error," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 14_18, Mar. 2011.

[6] Y. Liu, M. Hu, X. Ma, and H. Zhao, ``A new robust data hiding method for H.264/AVC without intra-frame distortion drift," *Neurocomputing*, vol. 151, pp. 1076_1085, Mar. 2015.