IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Encryption and Watermarking Embedded in H.264/AVC Video Stream

Sowmya Keerthi .D[1], Dr. K. Satya Prasad[2]

Department of ECE, University College of Engineering, JNTUK, Kakinada, India[1]

Professor, Department of ECE, University College of Engineering, JNTUK, Kakinada, India [2]

Abstract: Now a days, there is large growth in multimedia applications such video conferencing, video telephony, stream video/audio online etc. There is a need to secure the data. While transferring the data it plays a major role in today's scenario. So in this paper we discuss about hiding the data and images in a video. We propose a data and image hiding schemes embedded directly in the encrypted version of H.264/AVC video stream which includes different parts of H.264/AVC video and data encryption, data embedding and data extraction. The embedded data and image in a video is reconstructed without knowing the original host video. The video properties are analyzed with the codewords of IPMs, the codewords of MVDs, and the codewords of residual coefficients. Data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size should be preserved even after encryption and data embedding. We represent examples of embedding image and data in a video. We also discuss about different hiding techniques which include watermarking, steganography, cryptography.

Keywords: Data hiding, Encrypted domain of H.264/AVC, watermarking, codeword substituting, image encryption.

I INTRODUCTION

In today's daily life video is a common form of entertainment and these are complex than audio and images. There are various methods in adding or hiding secret data in audio, video or both. There are different technologies which provide the high efficient computation and large scale storage solution for video data is cloud computing. In cloud networking the security of data is critical and it is very important to maintain the confidentiality, integrity and the availability over the cloud network in order to improve the security and privacy concerns with cloud computing .

We propose the method of data hiding in the group of pictures or video frames and embedding it in video as cover. The data embedded in the video frames is encrypted using chaos encryption with secret key. Thus we provide the dual security for the data hiding and so no one can receive the data except the receiver. It becomes very difficult to attacker to detect or receive the secret data. However, for the requirement of application, it is necessary to perform data hiding directly in the encrypted domain. The most widely used data hiding technique for video is H.264/AVC (advanced video coding), gives the higher efficiency in video encoding by codeword substitution .This embedding of secret data directly in a video is compressed and then encrypted in H.264/AVC bit stream.

The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content by analysing the property of H.264/AVC codec, the code words of IPMs, code words of MVDs, code word of Residual Coefficients are encrypted with a stream cipher.

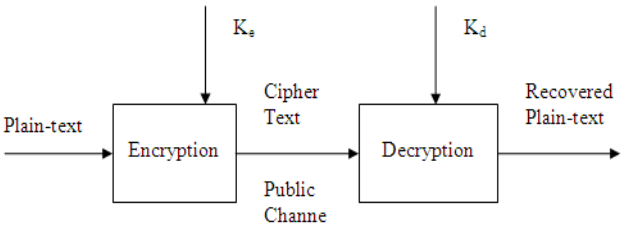

Fig 1. Encryption and Decryption Procedure of Data

Encryption is the method of changing the original data into a cipher text. Encryption deals with protecting the data by masking it. The input data for encryption is called plaintext which is denoted as P, and the encrypted data is called cipher-text, which are denoted as C.

The Encryption of a cipher text is given as C=Eke(P), where Ke is the Encryption key. Similarly, the Decryption of plain text is P=Dkd(C), where Kd is the Decryption key. When Ke=Kd, the cipher is called a PRIVATE-KEY CIPHER or a SYMMETRIC CIPHER .In private key ciphers, the encryption-decryption key must be transmitted from the sender to the receiver through a secret channel. When Ke=!Kd, cipher is called a PUBLIC-KEY CIPHER or an ASYMMETRIC CIPHER. .In public-key ciphers, the encryption key Ke is public, and the decryption key Kd is kept secret, there is no secret channel needed for key transfer.

Image encryption has a wide demand for real-time secure transmission of data. In image encryption algorithm, the data encryption standard (DES) has the low efficiency when the image is large. So, the chaos-based encryption has been suggested for an efficient way to deal with the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

problems, fast and provide high secure for image encryption. Chaos systems contain many properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most of these properties meet some requirements such as diffusion and mixing in the sense of cryptography.
Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. Crypto techniques ensure that the information being transmitted is not modified in the transmitter level. There is some difference in cryptography and steganography, in cryptography the hidden message is always visible, because information is in plain text form but in steganography hidden message is invisible. As the development of multimedia and Internet technologies, more information including images, audio and other multimedia, are being transmitted over the Internet. Recently, the image encryption technologies based on chaos theory have been developed to overcome the disadvantages present in early encryption techniques.

The paper is organized as follows. In Section II, the Encryption of Data is reviewed .The Code word substitution and Chaos Cryptography is described in Section III. And then followed by Conclusion.

II ENCRYPTION OF DATA

Data hiding techniques have recently become important in a number of application areas. An effective data-hiding process embeds the data in a digital video by using the motion vector phase angle of the macro block in the inter-frame. This method can be applied to either compressed or uncompressed videos. The embedded data can be extracted directly without use of the original video sequences. Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. We proposed a method that encrypts the data with a crypto algorithm and then embeds the encrypted data in a cover file. By this we can improve the security of the data.
In Walsh-Hadamard transform image watermarking algorithm is used in the encrypted domain using Parlier cryptosystem.

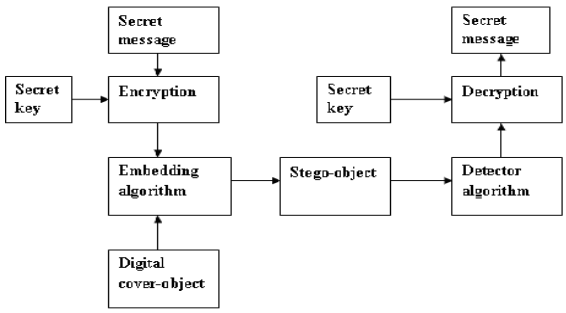

Fig2. Block Diagram of Encryption and Decryption Algorithm

This Parlier cryptosystem is based on the security requirements between buyer and seller. The encryption is performed by using bit-XOR operation.

To embed a secret data used two distinct methods:
(1) Encrypt the secret message
(2) The encrypted secret message is embed using Code word substitution technique.

A. ENCRYPTION OF VIDEO STREAM

The secret message is encrypted before embedding. This encryption method is simple and efficient, where only the secret key is known to receiver and sender The Secret key length is variable .At the receiver side during decryption , that is the reverse process of encryption carried out using the same key to obtain the secret message from stego medium .
Encryption of video often utilizes the time in an efficient manner in order to meet the requirements of real time applications. It is not desirable to compress and encrypt the whole video bit streams because of its compliance and computational cost. So, only some fraction of video data is encrypted to increase the efficiency and to achieve security. In order to satisfy the criteria we choose to encrypt three most important parts in the video. They are the intra Prediction Mode IPM, Moving Vector Difference MVD and the Residual Coefficients. To add a layer of improvement, the encryption is done after the encoding process. Selective encryption in H.264/AVC compressed domain has presented on Context-Adaptive Variable Length Coding (CAVLC), Context–Adaptive Binary Arithmetic Coding (CABAC).

- ENCRYPTION OF IPM:

Intra_4×4, Intra_16×16, Intra_chroma, and I_PCM are supported by the H.264/AVC standard, it is sufficient to encrypt only Intra_4 × 4, Intra_16×16. The macro block of the intra prediction mode (IPM), Intra_16×16 are encoded with Exp- Golomb code. This is followed by encryption which is bitwise XOR operation encoded code words with pseudorandom sequence from stream cipher.

- ENCRYPTION OF MVD:

Encryption of motion vector is preferred to guard the motion information along with texture information; The difference of the motion vector is obtained by the prediction on the vector. Thus obtained MVD is encoded by Exp-Golomb entropy coding.

- ENCRYPTION OF RESIDUAL DATA:

As high security is very important in which the residual data, in both I-frames and P-frames has to be encrypted. On analysing the standard of H.264/AVC, CAVLC entropy coding is suited to encode the quantized coefficients of a residual block.

B. WATERMARKING

A watermark is a image or pattern that appears in various shades of lightness/darkness in paper when viewed in light The watermark can be defined as an information that

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

is embedded into an image or a video for, providing security to the ownership.

The difference between information hiding and watermarking is the absence of an active operator. In watermarking, copyright protection and authentication of files or data, has an active operator that would attempt to remove. In information hiding there is no such active operator so there is no act of extracting the information hidden in the content, there by information hiding techniques need to be robust against accidental distortions

There are two methods in watermarking technique called as watermarking embedding and extraction system. Watermarking is of two types-visible watermarking and invisible watermarking. Visible watermarking refers to information visible on the file. Invisible watermarking makes information embed in a digital data. It is mostly used everywhere and can be retrieved quite easily.

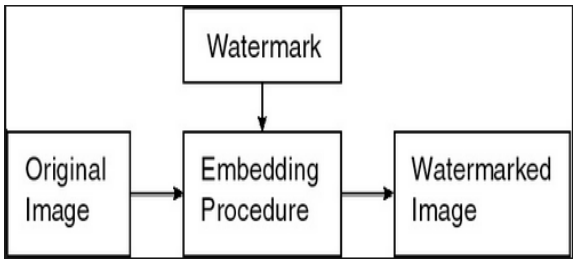

Fig 3.Block Diagram of Watermark

1. Applications:
- Used for copyright protection
- Used for tracing of source
- Used for photographs annotation Watermarking
- Usage-Specific Requirements
- Used for Fingerprinting
- Automatic Playlist Generation for Rights Verification
- Multimedia Authentication

1. Watermark Embedding
The eyes of human are more sensitive to noise in lower frequency range than **in** high frequency range , because the energy of original image are concentrated on the lower frequency range, and therefore, the quantization applied in lossy compression always reflects the human visual system sensitive to noise at higher frequencies.

To prevent hackers from extracting the secret information directly from the transformed domain, the watermarks are embedded to modify the relationship of the neighboring blocks of frequency coefficients of the original image instead of embedding by an additive operation. The original image is divided into 8 X 8 blocks of pixels, and the 2-D DCT is applied independently to each block. A 2-D sub-block mask is used to compute the residual pattern from the chosen frequency. Let the digital watermark be a binary image. A 2-D pseudo random number traversing method is used to permute the watermark so as to disperse its spatial domain.

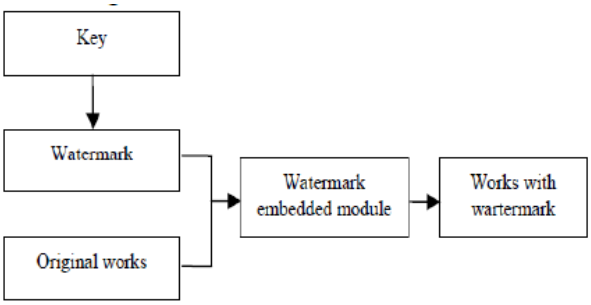

Fig 4.Procedure for Watermark Embedding

2. Watermark Detection
The detection of watermark requires the original frame, the watermarked frame and also the digital watermark. First of all the original image and input image are decomposed into regions of 128*128 both the original frames and the watermarked frames are transformed by DCT. To obtain residual values we make use of the frequency coefficients and the residual mask. Perform the XOR operation of two residual patterns to obtain a permuted binary signal. Reverse both the blocks and the pixel-based permutations to get the extracted watermark .Five watermarks are extracted by comparing the intensity pixel values of each region in the original frame with the watermarked frame

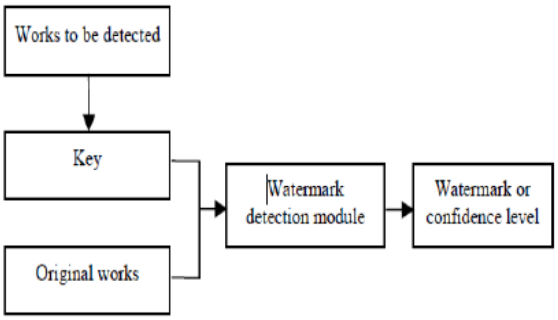

Fig 5. Procedure for Watermark Detection

C. WATERMARKING TECHNIQUES

Watermarking is a method of embedding the secret information into the digital media using some appropriate algorithm. It plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can destroy or detect the hidden information if he knows the algorithm otherwise it is critical to find out the watermark.

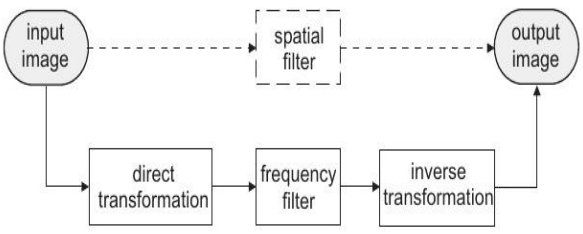

Fig 6. Brief Idea of Spatial and Frequency Domain

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

There are various algorithms used to hide the information. Those algorithms are of two domains, Spatial and Frequency domain

i. Spatial Domain
Spatial domain directly load the raw data into the original image. It can also be applied using colour separation. The watermark appears in only one colour bands. This shows that the watermark is difficult to detect under regular viewing. Spatial domain is changes an image representing an object in space to enhance the image for a given application. Techniques are based on manipulation of pixels in an image. Some of the algorithms of Spatial domain are:

a) Additive Watermarking:
The method for embedding the watermark in spatial domain is of adding pseudo random noise to the intensity of image pixels. The noise signals are integers or floating point numbers. To ensure the watermark detection, the noise is generated by a key, such that the correlation between the different keys will be very low.

b) Least Significant Bit:
The technique used for embedding the watermark is the LSB of pixels. Its easy to implement and does not generate any distortions to the image; however, it is not robust against attacks. The embedding of the watermark bits is performed by choosing an image pixels and substituting the least significant bit in each of the chosen pixels .The watermark may spread to the complete image or may be in the selected locations of the image. But these primitive techniques are vulnerable to attacks and can be destroyed easily.

c) SSM Modulation Based Technique:
Spread-spectrum techniques generate energy at one or more discrete frequencies and is spread or distributed in time. SSM based watermarking algorithm embeds information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

d) Texture mapping Technique:
This method is useful only to those images which can hide the watermark in the texture part of the image. This method hides data in the continuous random texture of images.

e) Patchwork Algorithm**:**
Patchwork is another technique for hiding based on a pseudorandom, statistical model. Patchwork inserts a watermark with a particular statistic using a Gaussian distribution.

ii. Frequency domain:
Frequency-domain methods are most commonly used, Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), are the reason for watermarking in the frequency domain. The human visual system (HVS) are captured by the spectral coefficients.

f) Discrete cosine transforms (DCT):
DCT represents data in terms of frequency space than an amplitude space. This is useful because it responds to the way humans perceive light, so that the non perceived part can be identified and removed away. DCT based watermarking techniques are robust ,to simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. They are difficult to implement and are computationally more expensive. At the same time they are weak to the geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking are classified into Global DCT watermarking and Block based DCT watermarking.

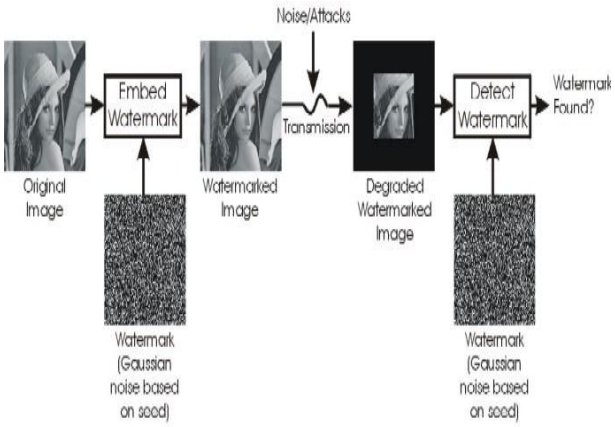

Fig 7. Watermarking process with Gaussian noise

g) Discrete wavelet transforms (DWT):
Discrete Wavelet Transform technique is widely used in digital image processing, compression, watermarking etc. The transforms are based on small waves called wavelet, which vary frequency at limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontally, vertically and diagonally. Magnitude of DWT coefficients is large in the lowest bands (LL) and at each level of decomposition its small for other bands (HH, LH, and HL).

The Discrete Wavelet Transform (DWT) is used in signal processing applications, like audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets are energy concentrated in time and are well suited for the analysis of transient, time-varying signals. The main challenge of the watermarking problem is to achieve a better trade off between robustness and perceptivity.

Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would also be increased. However, DWT is preferred because it provides both spatial localization and a frequency covered by the watermark within the host image.

DOI 10.17148/IJARCCE.2016.5884

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

D. STEGANOGRAPHY

The word steganography is arrived from Greek word steganos which means covered or secret and the graphy means writing or drawing which means "covered writing". It is the art of transmitting information through original files in a manner that the message existed in it is unknown. In simple words, it is hiding the information into a data or image or video. Steganography do not alter the message structure but hides inside a cover object. After embedding the secret message it is referred to as stego-medium.

A stego-key is used to control the hiding process so as to detection and/or recovery of the embedded data. Steganography and cryptography are different techniques. While cryptography is about protecting the content of messages. Steganography hides the information and cryptography protects the information. Due to hidden or invisibility it is difficult to recover hide information by the intermediate person. Procedure to know the steganography technique is known as steganalysis.

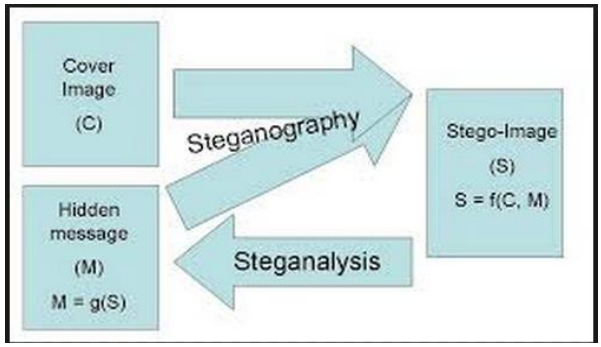

Fig .8 Block diagram of Steganography

Steganographic method following three main properties Capacity- The amount of the secret data to be hidden without significant change in the cover image. Robustness- The resistance for possible modification
Invisibility- The existence of the secret data can't be notified by anybody except receiver.

Some of the basic term used in steganography:
Message: information which is used to hide into images.
Cover-object**:** It refers to the embed message which is embedded in a message or an image.
Stego-object: Object which carrying a hidden message.
Stego-key: A key refers to a password used to hide and later retrieval of message.
Embedding algorithm: An algorithm used to hide the message.
Extracting algorithm: An algorithm used to recover the message.

E. TECHNIQUES OF STEGANOGRAPHY

They are many embedding techniques proposed by steganography. These techniques modify the cover-image with different approaches.. All the popular data hiding methods can be divided into two major classes: spatial domain and transform domain.

i. Spatial Domain

Spatial domain techniques embed information in the intensity of the original image. Basically,least significant bit (LSB) method is used where it replaces the least significant bit of original pixel with the message bit.

ii. Transform Domain

Transform domain also known as frequency domain where images are first transformed then the message is embedded in the image. Discrete cosine transformation (DCT) technique is used in JPEG images to achieve compression. DCT is a lossy compression transform where the cosine values cannot be generated as original; DCT changes values to hide the information.

F. CRYPTOGRAPHY

Cryptography is the study for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the various aspects in information security such as data confidentiality, data integrity and authentication. Modern cryptography intersects the mathematics, computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

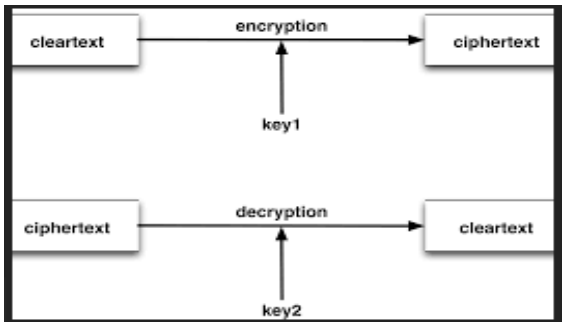

Fig 9.Process of Cryptography

Now-a-days cryptography was an effective synonym for encryption. The originator of an encrypted message shared the decoding technique needed to recover the original information with the intended recipients. Methods used to carry out cryptology have become increasing complex and its application more widespread .cryptographic algorithms are designed around computational hardness assumptions.

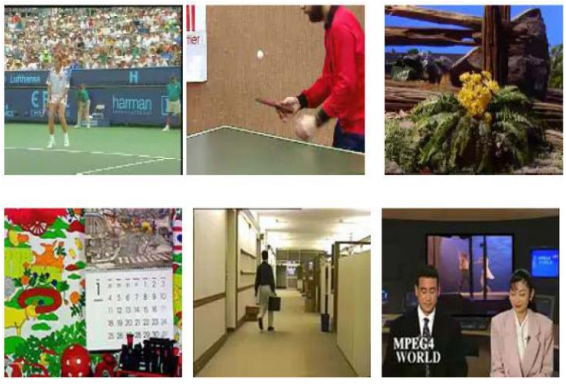

Fig 10 .Original Video Frames

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Fig 11.Encrypted Video Frames

Fig 12. Encrypted video frame with the encrypted data hidden

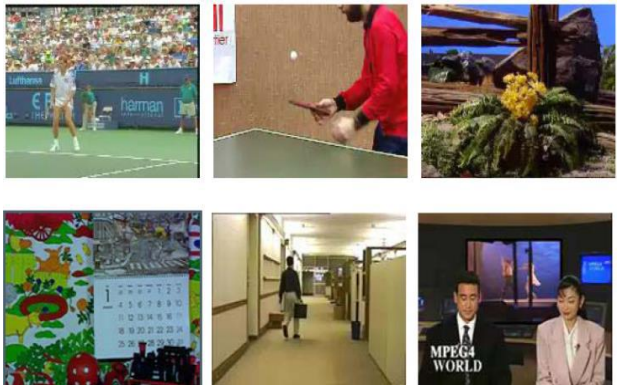

Fig 13. Decrypted Video Frame

III CODEWORD SUBSTITUTION

The previous method performs encryption and data embedding simultaneously during H.264/AVC compression phase. Hence the compression and decompression cycle is the time consuming and it affects real time implementation

Data hiding performed entirely in the encrypted domain preserves confidentiality of the content during cloud storage. The technique operates directly on the compressed bit stream. In order to adapt to various application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

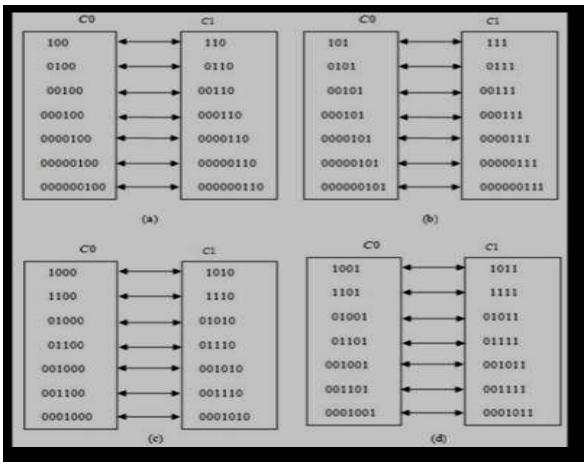

Fig 14. Codeword Mapping for CAVLC

The code words substitution should satisfy the following limitations:

- First, the bit stream after codeword substituting must remain syntax compliance so that it can be decoded by standard decoder.
- Second, to keep the bit-rate unchanged, the substituted codeword should have the same size as the original codeword. The code words of Levels which suffix Length is 2 or 3 would be divided into two opposite code spaces denoted as C0 and C1 as shown in Figure 14.
- The code words assigned in C0 and C1are associated with binary hidden information "0" and "1".

G. CHAOS CRYPTOGRAPHY

Chaos systems is suitable for data message encryption

1) Chaos motion is neither periodic nor convergent, and the domain is limited. With time passing, the points of the movement trace traverse all over domain.

2) Flexing and collapsing are carried continually through the limited domain. Therefore the outputs of chaotic systems are very irregular, similar to the random noise.

The discrete sequences of the chaos dynamical system are gained by the following equation.

$Xn+1 = Tn(xk)$.

The basic Logistic-map is formulated as,

$f(x)=\mu x(1-x)$

Where, x (0, 1). The parameter μ and the initial value x0 can be adopted as the system key (μ, x0). The research result shows that the system is in chaos on condition that $3.569 < \mu < 4.0$.

IV CONCLUSION

Data hiding in encrypted video is a new technology that has started to cause attention due to the storage and privacy requirements from cloud server network. There are infinite number of steganography applications for digital image including copyright protection, feature tagging, and secret communication. This paper explores a tiny fraction of the art of watermarking and steganography. An algorithm to embed additional data in

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

encrypted H.264/AVC bit stream is presented, which includes the video encryption, data embedding and data extraction stages. The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e., it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications The steganography method may be further secured if we compress the secret message first and then encrypt it and then finally embed inside the cover file.

REFERENCES

[1.] Digital watermarking and other data hiding techniques International journal of innovative technology and exploring engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April-2013
[2.] A new spatial domain algorithm for gray scale images watermarking Proceedings of the international conference on computer and communication engineering 2008, May 13-15, 2008, kuala lumpur, Malaysia
[3]. Xiping He Qionghua Zhang, **"**Image Encryption Based on Chaotic Modulation of Wavelet Coefficients", Congress on IEEE Image and Signal Processing (CISP'08), Sanya, Hainan, Vol.1, pp.622-626, 27- 30 May 2008
[4]. Babloo Saha, Shuchi Sharma (2012), "Steganographic Techniques of Data Hiding Using Digital Image", vol. 62, pp. 11-18
[5]. DawenXu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014.
[6]. W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Acouist., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.
[7]. W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012

BIOGRAPHIES

Dr. K. Satya Prasad, Awarded with 13 Ph. D scholars currently working as Professor of ECE Department with 38 years of teaching experience and 20 years of R&D experience. His Area of interests include signals &systems, DSP, communications and Radar telemetry.

D. Sowmya Keerthi received a B.Tech Degree under the stream of ECE from Kakinada Institute of Engineering and Technology for Women. Currently pursuing M.Tech in Jawaharlal Nehru Technological University Kakinada under the department of Electronics and Communication Engineering.