PROTECTION FOR ENCRYPTED DATA AND LOGO IN H.264/AVC VIDEO STREAMS BY CHAOS

D.Sowmya Keerthi
Department of ECE
University College of Engineering JNTUK
Kakinada ,India .
Sowmyarthi@gmail.com

Dr.K.Satya Prasad
Department of ECE
University College of Engineering JNTUK
Kakinada ,India.

Abstract— **Digital videos are to be stored, processed and transmitted in the encryption of compressed video bit streams in order to maintain security . Data has to be hidden in these encrypted videos for the purpose of content notation and tampering detection. Data hiding without decryption preserves the confidentiality of the content more efficiently .Data hiding is the encrypted version of H.264/AVC video streams which includes three parts i.e., data embedding ,data extraction,H.264 /AVC codec . The code words of intra prediction modes, motion vector differences ,and residual coefficients are encrypted with stream cipher in H.264/AVC codec. By using bit replacement technique ,A data hider can embed additional data in the encrypted domain without changing or knowing the original video content .The proposed approach presents the selective encryption ,and Data hiding in LSB process .We propose Chaos Crypto System to encrypt /decrypt the secret info before/after the embedding/extraction of info. This process is used for reducing time consumption, avoids leaks of videos ,better compatible for privacy protection**

Keywords— Bit replacement technique ; Chaos crypto system ; Data hiding in Encrypted bit stream ; H.264/AVC.

I. INTRODUCTION

Data hiding and watermarking in digital videos have wide literature. Cloud computing is an important technology ,providing high efficiency in computation and large scale storage of video data .These cloud services have many attacks and are vulnerable ,so these videos are to be encrypted and then stored on cloud ..The ability of performing data hiding in encrypted H.264/AVC video streams would avoid the leakage of video content , this helps in security and privacy concerns.

Data hiding is the process of embedding information into a host medium. Data hiding in videos are of two ways: bit stream level and data level. In bit stream level ,the redundancy with the compression standards are exploited and have various options to the encoder during encoding .Where as, data level are more robust to attacks and suitable for broad range of applications. This type of hiding the data is helpful for fragile applications ,such as authentication. Data Hiding is the method of embedding information secretly inside a cover media without altering its perceptual quality. Data Hiding differs from cryptography, but utilizes some of its basic concepts.

Pure data hiding simply embeds the data without encryption. A Secret key is used to encrypt the data that has to be hidden by using the common keys between the end users. In data-hiding method the receiver needs only to process the required steps sent in order to retrieve the message. If not the existence of the hidden information is virtually undiscoverable. Thus a combination of cryptography and steganography can be used for hiding the secret data. The secret data can be any form of media. Any form of media file that is chosen to be hidden in the encrypted video has to be converted into a binary format so that it can be embedded in a better way..

A cloud server can embed the information into an encrypted H.264/AVC video by using data hiding technique .The encryption process of video mainly be classified into four unique ways of encrypting the data. The *FULLY LAYERED* ENCRYPTION PROCESS deals with the encryption of each and every byte. This encryption increases the computation their by the speed is increased. Another method which is used to scramble the content is *PERMUTATION BASED ENCRYPTION* methods .*SELECTIVE ENCRYPTION* which is widely used encrypts only some key features in the video. *PERCEPTUAL ENCRYPTION* the content encrypts partially, selective encryption does not give any perceptual track of the original video.

The server can manage the video and cross check the integrity without knowing the original content ,this process helps in security and privacy protection. This technology can be used for surveillance videos or medical videos that have been encrypted for protecting the privacy of the people .The data base manager can add the personal information into the corresponding video to provide management capabilities in the encrypted domain. H.264/AVC video encryption scheme are encrypted with stream cipher to meet the requirements to real time applications. Its not able to encrypt the whole compressed video bit stream like traditional cipher does ,because of computational costs only a fraction of video data is encrypted to increase the efficiency and to achieve security .The encryption algorithm is a combination of EXP-GOLOMB ENTROPY CODING and CONTEXT – ADAPTIVE VARIABLE LENGTH(CALVC) where the code word length is unchanged .

II. PROBLEM FORMULATION

Till now ther are many data hiding schemes in the encrypted domain..Information hiding techniques have recently become important in our daily lifes and in many areas. In a watermarking scheme the encrypted domain usin Paillier cryptosystem is proposed based on security requirements of buyer-seller watermarking protocols.In a Walsh –Hadamard transform based image watermarking algorithm in the encrypted domain using paillier cryptosystemis present .Digital audio ,video pictures are increasingly furnished with distinguishing marks ,which may contain a hidden copyright noticeor even helpto prevent the unauthorized copying directly**.**

Military communications system make use of traffic security techniques ,which they merely concealing the content of a message using encryption ,seek to conceal its sender ,its receiver .Similar techniques are used in medical surveillance and in some mobile phone systems . The encryption is performed by using bit –XOR operation. In these methods the original image is in an uncompressed format .In a robust watermarking algorithm is proposed to embed watermark into compressed and encrypted JPEG2000images. Now –a –days the multimedia and internet technology has been developed ,more information with images ,audios and videos are being transmitted over Internets .Recently ,the image and data encryption technologies based on chaos theory has been developed to overcome the disadvantages present in the early techniques.

A. *Watermarking*

The watermark can be defined as an information that is embedded into an image or a video for, proving security to the ownership It is used to verify the identity of the owner and thereby create a copyright protection for the file. It is a recognizable image or logo that appears in various shades of lightness/darkness .There are two steps in watermarking technique called as watermarking embedding and extraction system.

Watermarking can be mainly classified into two types-visible watermarking and invisible watermarking. There are two main ways of producing watermarks on paper : the dandy roll process and the cylinder mould process

i. Visible watermarking

This refers to information visible on the file.

ii. Invisible watermarking

It makes information embed as a digital data. It is mostly used everywhere and can be retrieved quite easily

.

iii. Dandy Roll Process

The *dandy roll* is a light roller covered by material similar to window screen that is embossed with a pattern. Faint lines are made by LAID WIRES that run parallel to the axis ,and the bold lines are made by CHAIN WIRES that run around the circumference to secure the laid wires from the outside.

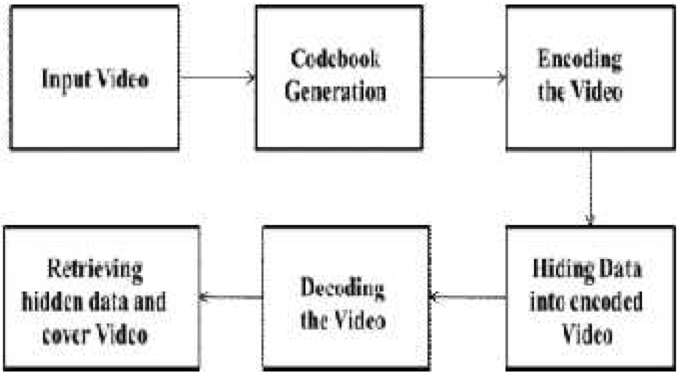

Input Video
Codebook Generation
Encoding the Video
Hiding Data into encoded Video
Decoding the Video
Retrieving hidden data and cover Video

Fig**.** 1 Block Diagram of Proposed Method

iv. Cylinder Mould Process

The cylinder mould process , is a shaded watermark created by areas of relief on the roll's own surface. Once dry, the paper may then be rolled again to produce a watermark of even thickness but with varying density. Cylinder Mould Watermark Paper is the preferred type of watermarked paper for banknotes, passports, motor vehicle titles, and other documents where it is an important anti-counter fitting measure.

B. *H.264/AVC Encryption*

The mostly used standard for video is H.264/AVC(Advanced Video Coding)which provides the higher efficiency in encoding the video . The H.264/AVC design allows encoders to make the following decisions when coding a frame.

1) To combine the two fields together and code them as one single coded frame

2) We do not combine the two fields and code them as separate coded fields

3) To combine the two fields together and compress them as a single coded frame, but while coding the frames to split, the pairs of two vertically adjacent macro blocks are either paired of two field or frame macro blocks before coding them.

Data hiding directly in H.264/AVC video stream would avoid the leakage of video content .In this H.264/AVC codec ,the codeword of intra prediction modes ,the code word of motion vector differences and the codeword of residual coefficients are encrypted with stream cipher. The data extraction can be done either at the encrypted domain or in the decrypted domain .The size of the video file is preserved even after encryption and data embedding .But in practical cases the whole video cannot be compressed into bit stream due to format compliance and cost .So, only a fraction of video is encrypted and data is embedded in that to improve the efficiency and security .The encrypted bit stream can be decoded by any standard complaint H.264/AVC decoder ,but the encrypted video data is treated completely different to plain text. H.264/AVC encrypt three most important parts in the video. They are the Intra Prediction Mode (IPM) , Moving Vector Difference (MVD) and the Residual Coefficients. For the security , the encryption is done after the encoding process.

- ***Encryption of IPM***

There are different intra prediction modes available Though Intra_4 × 4, Intra_16×16, Intra_chroma, and I_PCM are supported by the H.264/AVC standard,. In these modes only Intra_4 × 4, Intra_16×16can be encrypted . .The luminance block of , Intra_4 × 4 is used for the spatially neighboring samples macro block type of , Intra_16×16 is encoded with Exp- Golomb code

- ***Encryption of MVD***

To protect the motion information along with texture information,. The difference of the motion vector is obtained by the prediction on the vector. The MVD obtained is encoded by Exp-Golomb entropy coding. In the Exp-Golomb coding the last bit of the codeword is encrypted by X-OR operation with pseudorandom sequence .

- ***Encryption of RESIDUAL DATA***

For the high security purpose we take another another sensitive data, which is the residual data, in both I-frames and P-frames which has to be encrypted. In H.264/AVC,CAVLC entropy coding is used for encoding of residual blocks.

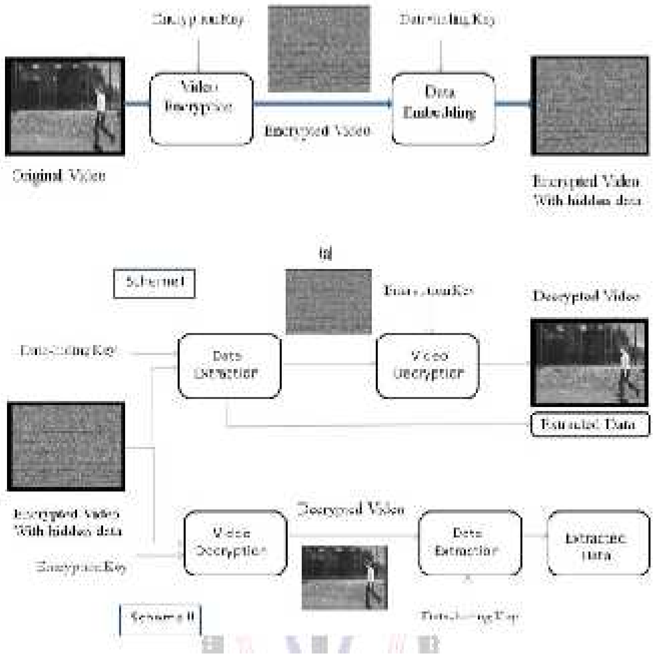


Fig.2 Block diagram (a) video encryption and data hiding at sender side (b) data extraction by two schemes at receiver side

C. Data Embedding

The H.264/AVC encrypted video bit stream , proposed the data embedding is done by codeword substitution technique. The sign of Levels encrypted by the desired data hiding should not be affected.

The code words substitution should satisfy the following three limitations, Firstly, the bit stream after substituting the codeword must remain with same syntax compliance so that it can be decoded by standard decoder. Secondly, the size of the substituted codeword should be same as that of the original codeword so as to keep the bit rate unchanged Third, visual degradation impact occurred by data hiding should be minimized . That is the data which has been embedded into the video has to be visible to human observer in the decryption side .

- ***Data hiding algorithm***

```
Input: Video
Output: Stego video
Step 1: Read the input Video
Step 2: Perform frame seperation
Step 3: Apply H.264/AVC to compress the frame.
Step 4:Apply secret key to hide the data.
Step 7: Apply chaos encryption Algorithm to embed data
Step 8: Generate Stego video
```

D. Data Extraction

The hidden data can be extracted either in encrypted or decrypted domain, as shown in Fig.2(b).

1)Scheme I: ***Encrypted Domain Extraction***.

To maintain privacy, a database manager (e.g., cloud server) can only get access to the data hiding key and have to manipulate the data in encrypted version of the video .For that purpose the data extraction in encrypted domain guarantees the feasibility of proposed scheme. In encrypted domain, as shown in Fig. 2(b), encrypted video with hidden data is directly sent to the data extraction module, and the extraction process is done further.

2)Scheme II: ***Decrypted Domain Extraction***.

Both the embedding and extraction of the data are performed in encrypted domain .But in some case, user wants to decrypt the video first and then extract the hidden data from the decrypted video. For example, an authorized user, who owned the encryption key, has received the encrypted video with a data hidden . The received video can be decrypted by using the encryption key only , that means, the decrypted video still includes the hidden data, which can be used to trace the source of the data. Data extraction in decrypted domain is suitable for such case. As shown in Fig. 2(b), the received encrypted video with hidden data is first pass through the decryption module and then data extraction is done.

The step by step process of decryption and data extraction is as follows.

Step1: The video encryption streams are generated with the encryption keys as given in the process.

Step2: The code words of IPMs, MVDs, Sign-of-Trailing Ones and Levels are identified by solving the Encrypted bit stream.

Step3: The decryption process is same as the encryption process, since XOR operation is symmetric. By performing XOR operation to encrypted code words the decryption is achieved ,as the two XOR operations cancel each other which gives the original plain-text. Since the video encryption streams depends on the encryption keys, the decryption is possible only for the authorized users. After generating the decrypted code words with hidden data, the content owner can further extract the hidden information.

Step4: The last bit encryption may change the sign of Level. The encrypted codeword and the original codeword
are still in the same code spaces. If the decrypted codeword belongs to code space C0,then the hidden data bit is "0",if it belongs to C1, then the hidden data bit is "1".

Step5: Generate the same pseudo-random sequence which is used to hide the data .The extracted bit sequence should be decrypted to get the original additional information

- ***Data Extraction algorithm***

```
Input: Stego video
Output: Hidden data
Step 1: Read Stego video.
Step 2: Perform decoding using reverse chaos decryption
Step 3: Extract hidden data using code word substitution and Secret Key.
```

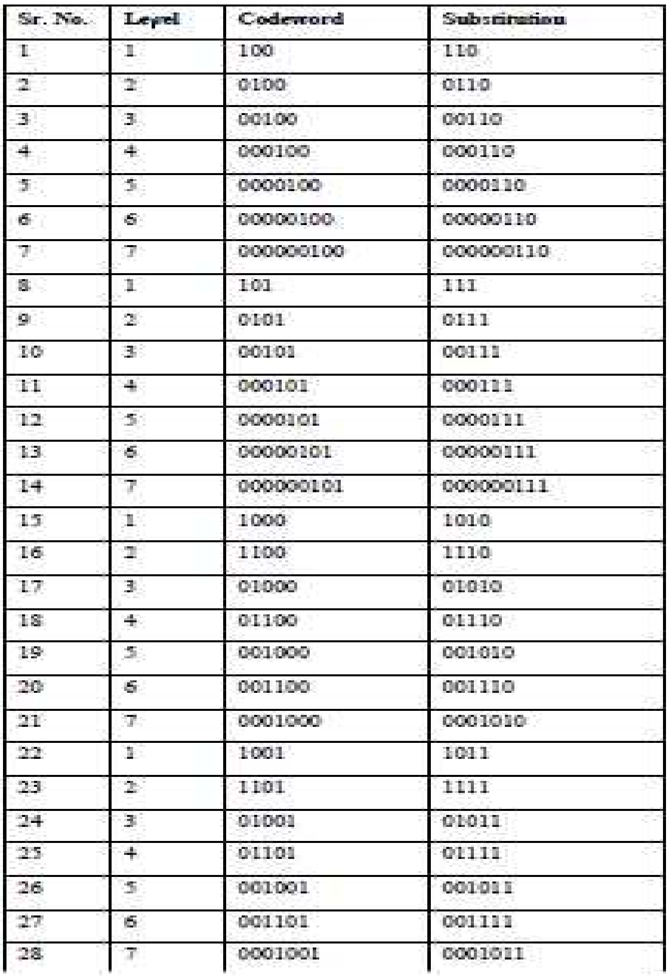
E. Data Security

In this encryption methods IPM, MVD and residual coefficients are used which keeps perceptual security for the encrypted video. This technique gives cryptographic security and perceptual security. At the same time for enhanced security purpose we can use the key for encryption and decryption process, so that unauthorized person cannot access the video file or data.

- ***Secret key generation algorithm***

```
Step 1: Take a key which is a prime number(for exp)
Step2: Generate two prime numbers p, q nearer to given key.
Step3: Calculate n=p*q;
Step 4: Calculate m= (p-1)(q-1).
Step 5: Generate e ,Assume e=1; x=1;
        While (mod(m , e)==0)
         e = e+1;
Step 6: Generate d ,Take s=1+x*m;
        While (mod(s , e) ~= 0)   x = x+1;  s=1+x*m;
```

TABLE 1. Code word Substitution



Sr. No.	Level	Codeword	Substitution
1	1	100	110
2	2	0100	0110
3	3	00100	00110
4	4	000100	000110
5	5	0000100	0000110
6	6	00000100	00000110
7	7	000000100	000000110
8	1	101	111
9	2	0101	0111
10	3	00101	00111
11	4	000101	000111
12	5	0000101	0000111
13	6	00000101	00000111
14	7	000000101	000000111
15	1	1000	1010
16	2	1100	1110
17	3	01000	01010
18	4	01100	01110
19	5	001000	001010
20	6	001100	001110
21	7	0001000	0001010
22	1	1001	1011
23	2	1101	1111
24	3	01001	01011
25	4	01101	01111
26	5	001001	001011
27	6	001101	001111
28	7	0001001	0001011

F. Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Its mostly constructed and analyzing protocol that the influence of adversaries are overcome in many aspects of security. Its has many applications in daily life and also intersects the disciplines of computer science and electrical engineering.

The important elements in cryptosystems are
1. Plain text (input)
2. Encryption algorithm
3. Secret key
4. Cipher text
5. Decryption algorithm

Mainly divided into two types-

- ***Public key cryptography*** (asymmetric cryptography)-it contains two keys one is secret key and the other is public key

- ***Symmetric cryptography***-It contains same key to perform both .

III. EXPERIMENTAL RESULTS

H.264/AVC video bit stream has proposed data hiding with video compression .The GOP (Group of Pictures) structure is "IPPPP: one I frame followed four P frames". These IPPPP frames are used to embed the data in the video.

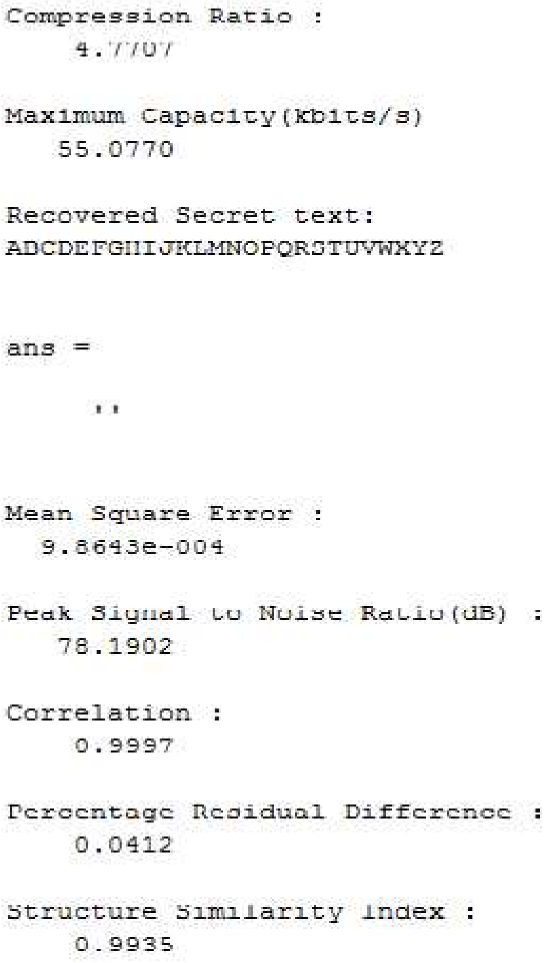
- ***Encryption Algorithm Security***

The security includes both cryptographic and perceptual security. *Cryptographic security* means the security against the attacks of cryptographic ,which depends on the ciphers text adopted by the scheme. In the proposed scheme, the secure stream cipher in the encrypted bit stream and chaotic pseudo-random sequence generate a logistic map that is used to encrypt the additional data and provide security against cryptographic attacks. *Perceptual security* refers to the encrypted video which is unintelligible or not. It depends on the encryption properties. In case of encrypting ,only IPM cannot keep secure enough, since the encrypted video is intelligible. The proposed scheme encrypts IPM, MVD and Residual Coefficients, which keeps perceptual security of the encrypted video. The high-motion videos with perceptual quality complex textured background becomes more scrambled after encryption than that of the low-motion videos with a static background. That 's because of less residual coefficients and MVD's in videos that are available for encryption. In general, scrambling performance of the encryption system is more than adequate.

- ***Stego Video Visual Quality***

The encrypted video containing hidden data provided by the server should be decrypted by the authorized user. the visual quality of the decrypted video containing data hidden is expected to be equal to the original video. In this only the code words of Levels within P-frames are modified for data hiding. Simulation results have demonstrated that we can embed the additional data with a large capacity into P-frames while preserving high visual quality.

PSNR(Peak Signal to Noise Ratio),SSIM(Structural Similarity Index) and VQM(Video Quality Measurement) are adopted to evaluate the perceptual quality of the encrypted video. ***PSNR*** is used mostly in objective video quality metric and does not correlate perfectly to the visual quality due to nonlinear behavior of human visual systems. ***SSIM*** lies in between 0and 1 ,where 1 indicates the host image which is identical to the stego image(target image).H.264/AVC is a lossy compression so the data hiding of visual quality of non stego video stream should be tested .The decompressed non-stego video stream is a target image ,while the original uncompressed video sequence is a reference image. The target video or image contains a hidden data . The ***VQM*** is another method to measure video quality ,it correlates more with the human visual system. The low VQM value the high perceptual video quality if it extends to zero that indicates excellent quality. The higher ***QP***(Quantaization Parameter) results in lower video quality



```
Compression Ratio :
     4.7707

Maximum Capacity(Kbits/s)
    55.0770

Recovered Secret text:
ABCDEFGHIJKLMNOPQRSTUVWXYZ


ans =

      ''



Mean Square Error :
  9.8643e-004

Peak Signal to Noise Ratio(dB) :
    78.1902

Correlation :
     0.9997

Percentage Residual Difference :
     0.0412

Structure Similarity Index :
     0.9935
```

- ***Chaos crypto system method***

The chaos systems are suitable for data encryption because the chaotic motion is neither periodic nor convergent and the domain is limited .The flexing and collapsing of crypto system are carried continually through the limited domain. The output of chaotic system are very irregular,similar to the random noise. The discrete sequences of the chaotic system is gained by Xn+1 = Tn (xk).

The basic Logistic-map is given as *f*(x)=μx(1-x) Where, x(0,1). The chaos crypto parameter μ and the initial value x0 can be adopted as the system key (μ, x0). The chaos ranges that 3.569 < μ < 4.0.

- ***Bits Replacement Technique***

The frequently used steganography method is LSB substitution technique . Every pixel of gray-level image consists of 8 bits. One pixel can display 28 =256 variations. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly.

IV. CHAOS METHOD RESULTS

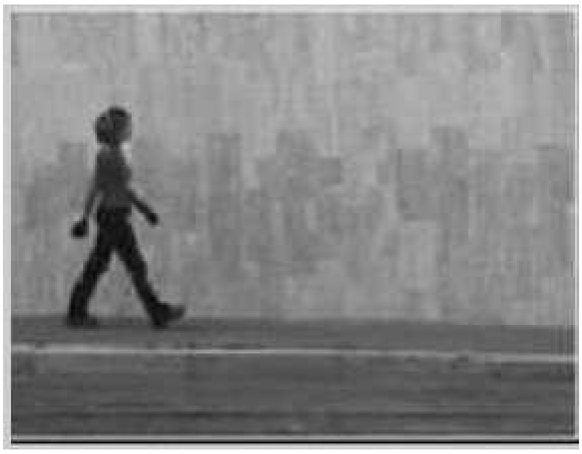


Fig.3 Reconstructed video image with data and logo hidden in it .

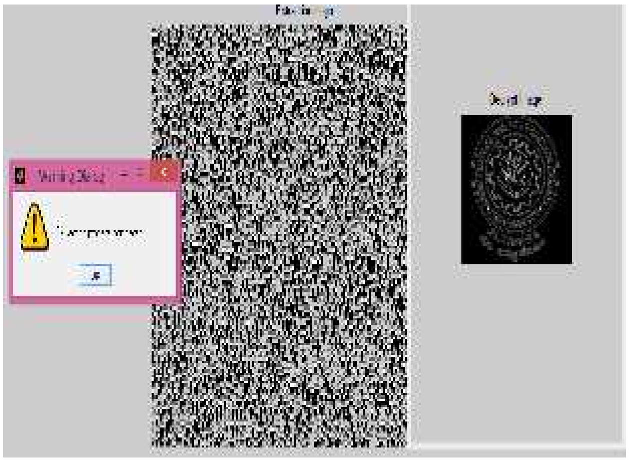


Fig 4. Extracted logo from the reconstructed video and the decrypted image is shown

V. CONCLUSION

Data embedding in the encrypted domain is drawing attention in today’s world attention. In this paper, data is encrypted by H.264/AVC bit stream, which includes the video encryption, data encryption ,and Image or logo encryption by using chaos method, data embedding and data extraction . 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,

The data-hider can embed additional data into the encrypted bit stream using codeword substitution, even though he does not know the original video content Here data is first encrypted and then embed in an image /logo with help of code word substitution , and that image goes through a chaos encryption and is embedded in the video. Furthermore the data hiding process is entirely in the encrypted domain, so can preserve the confidentiality of the content completely. With an encrypted video containing hidden data and image , data extraction can be carried out either in encrypted or decrypted domain, which provides different practical applications. The results are shown in the above fig 3 and fig 4

VI. REFERENCES

[1] 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

[2] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013

[3] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, “Robust watermarking of compressed and encrypted JPEG2000 images,” *IEEE Trans. Multimedia,* vol. 14, no. 3, pp. 703–716, Jun. 2012.

[4] W. J. Lu, A. Varna, and M. Wu, “Secure video processing: Problems and challenges,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[5] B. Zhao, W. D. Kou, and H. Li, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.

[6] 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.

[7] Xin Zhang, Weibin Chen, “A New Chaotic Algorithm For Image Encryption”, pp 889-892 IEEE ICALIP2008

[8] Dong enxeng, Chen Zengqiang, Yuan zhuzhi, Chen zaiping, “A Chaotic Images Encryption Algorithm with The Key Mixing Proportion Factor”,pp 169-174 Computer Society IEEE 2008.

[9] Chong Fu, Zhen-chuan Zhang, Ying-yu Cao, “An Improved Image Encryption Algorithm Based on Chaotic Maps”, Computer Society, IEEE 2007

[10] Shrutika S. Giradkar. Antara Bhattacharya, “Securing Compressed Video Streams using RC4 Encryption Scheme” Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015),IEEE 2015