Forbidden Zone Data Hiding in Video Using Selective Embedding Techniques

[1] N Manasa, [2] G Karunakar Goud [3] Prasad B
[1]II/IV, [2]Assistant Professor[3]Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM)
Hyderabad
[1] nagillamanasa7564@gmail.com [2], karna3009@gmail.com[3]bprasad@gmail.com

Abstract **Due to the design complexities involved the video data hiding is still an important research topic. We propose a new video data hiding method that makes use of erasure correction capability of repeat accumulate codes and superiority of forbidden zone data hiding. Selective embedding is utilized in the proposed method to determine host signal samples suitable for data hiding. This method also contains a temporal synchronization scheme in order to withstand frame drop and insert attacks. The proposed framework is tested by typical broadcast material against MPEG- 2, H.264 compression, frame-rate conversion attacks, as well as other well-known video data hiding methods. The decoding error values are reported for typical system parameters. The simulation results indicate that the framework can be successfully utilized in video data hiding applications. Data hiding is the process of embedding information into a host medium. In general, visual and arual media are preferred due to their wide presence and the tolerance of human perceptual systems involved. Although the general structure of data hiding process does not depend on the host media type, the methods vary depending on the nature of such media.**

Keywords: **Video data hiding, Forbidden zone data hiding, Compression, Frame-rate conversion attacks.**

I. INTRODUCTION

Steganography is the hidden communication domain. Using Steganography, a secret message is grafted onto a medium such as a picture, audio and in video clip and sent. Then that hidden message is not known, except for the sender and receiver. The word is derived from Greek words meaning covered and graphia stegos write meaning. There are a number of uses of Steganography. The cryptography and Steganography are associated; there is a difference between the two. Cryptography is used to clamber messages so that they cannot be understood. It does not deny the fact that the message exists. Steganography, on the other hand, hide the fact that the message exists by hiding the actual message in another [22].

One of the most used applications is digital watermarking. A watermark is the reproduction of an image, logo or text on the paper so that the source of the document can be at least partially authenticated. A digital watermark can perform the same function, a graphic artist, for example, can send sample images on their website complete with a signature later incorporated you can show your property if others try to portray their work as their own. Another technique of Steganography is Video i.e. to hide data in Video. One of the most popular tools that are often used to hide the data is called Slacker. Slacker breaks a file and places each piece of that file slack space for other files, thereby hiding from forensic analysis software. Another data hiding technique involves the use of defective sectors. To perform this technique, the user changes a particular sector from good to bad data and then placed in that particular group. The belief is that forensics tools see these groups as bad and continue without examining its contents.

Currently, Internet and digital media are becoming more and more popular. As a result, the requirement for secure data transmission also increased. Several good techniques are proposed and already have in practice. Data hiding is the process of incorporating information secret within a data source without changing its original quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and the recipient, even realizes there is a hidden message. In general, data hiding, the actual information is not kept in its original form and thus becomes an alternative equivalent multimedia file such as image, video or audio which in turn is concealed within another object. This manifest message is sent over the network to the recipient, where the real message is separated from it. It is the process of embedding information into a host medium. In general, visual and aural media are chose due to their presence and the allowance of human perceptual systems involved. Even though the general structure of data hiding process does not depend on the host media type, the methods change depending on the nature of such media. For example, image and video data hiding having many common points, therefore video data hiding continues to constitute an active research area.

The requirements of any data hiding system can be classified into safety, capacity and robustness. All these factors are inversely proportional to each other creating a dilemma called data hiding. The aim of this work is to maximize the first two factors of data hiding i.e. safety and capacity along with the detection of alteration.

The proposed scheme is a data hiding method that uses high-resolution digital video as a carrier signal. The proposed recipient only has to process the necessary steps in order to disclose the message. Otherwise the existence of the hidden information is virtually undetectable. The proposed scheme provides for a quality hide important information so it is different from the typical data hiding mechanisms because here we consider the application that require much larger loads, such as video and video on video image. The purpose of concealing that information depends on the application and the needs of the owner / user of digital media. Data hiding Requirements are:

- **Imperceptibility-** Video with the data and the original data source must be perceptually identical.
- **Robustness-** The embedded data should go through any processing operation the host signal and passes to preserve allegiance.
- **Capacity-** It Maximizes data payload of embedding.
- **Security-** Security is in the key.

Data Hiding is totally different concept to cryptography, but uses some of its basic principles. In this paper, we consider some important aspects of data hiding. Our consideration is to incorporate information on video that can survive the attacks of the network.

Data hiding is the integration of information in a host medium. In general, the media visual and auditory are preferred due to their wide presence and tolerance of human perception systems involved. While the basic structure of data hiding process is not dependent on the type of host media, methods change depending on the nature of such means. For example data, image and video hidden common shares many points. However concealed video data requires more complex designs, as a result of the additional time dimension. Therefore, the video data hiding remains an active research area.

Hiding data in video sequences is performed in two main ways: the bitstream level and data level. In bitstream-level redundancies within the current compression standards are exploited. Typically, coders have various options during encoding and this freedom of choice is suitable for the purpose of handling data hiding. However, these methods rely on highly structure of the bit stream, so they are quite fragile in the sense that in many cases cannot survive for any format conversion or transcoding, even without any significant loss of the perceptual quality. So, this type of data hiding methods is basically fragile proposed for applications such as authentication. Moreover, data-level methods are more robust to attacks. Therefore, they are suitable for a wider range of applications.

Despite its fragility, methods based on bitstream-remain attractive for data hiding. For example, in [4], the redundancy in the block size selection is exploited H.264 coding for hiding data. In another approach [5], the quantization parameter and the DCT (Discrete Cosine Transform) coefficients are altered in the bit stream level. However, most methods of video data hiding using uncompressed video data. Sarkar et. al. [6] proposes a large volume transform domain data hiding in MPEG-2 video. QIM apply to low frequency DCT coefficients and adapting the quantization parameter based on MPEG-2 parameters. Furthermore, fouling rate vary depending on the type of the frame. As a result, insertions and deletions occur in the decoder, which causes de-synchronization. They use Repeat Accumulate (RA) codes to withstand scratches. Since adjusting the parameters according to the type of frame, each frame is treated one by one.

***Selective Embedding*:**

Host signal samples, which will be used in data hiding, are determined adaptively. The selection is performed at four stages: frame selection, frequency band determination, block selection, and coefficient selection.

- **Frame selection:** Selected number of blocks in the entire frame is counted. If the ratio of the selected blocks in all blocks is above a certain value (T0) the frame is processed. Otherwise, this setting is ignored.

- **Frequency band:** Only certain DCT coefficients are utilized. Middle frequency band of DCT coefficients
- **Block selection:** Energy mask coefficient is calculated. If the energy of the block is greater than a certain value (T1) below, the block is processed. Otherwise, it is ignored.
- **Selection coefficient:** the energy of each coefficient compared to another threshold T2. If the energy is above T2, then used for embedding other data along with selected coefficients in the block.

II. SYSTEM ANALYSIS

Problem Definition:

Data hiding video is active research topic in these days. Due to high resolution and due to its complex design it is in one of the difficult task. Hiding data in images some other multimedia files is an easy task or easy procedure. Because to embed (add) some hidden bits in these is not difficult task, after embedding it is also easy to send this original data as well as hidden data which is embed in the original data over the network i.e. easy to send this data to receiver through a network. When receiver receive this data then it is also easy to decode or extract the hidden data from the original data. But when we talk about the Data that is hidden in the Video, that look or seem a very difficult task, because the size of video as compare to the size of the images and text files is large and also the complexity of the video as compare to the these files is larger. So, due to these parameter or these attributes, to hide data in video seems a tough task. When we hide data in AVI high resolution video, the size of this video is already big but when we add some extra bits or data that we want to send in hidden form, it will increase the comparative size or increase the size of video beyond its limit. So it is very destructive or worst idea to hide the data in Video. It also affects the quality of video when we try to hide in video. As a result the intruders easily sniff that there is something in the video, which directs it to loosen the security. Following are the main problems facing during the Hiding data in video - Complex Design, Size, Security and Quality

Objective:

The main objective and direct of this paper is to maintain the Quality, Size, Security and the design of video in the original form after the hiding of the data. There were some researches that try to maintain these parameters but they fail at some point. So in this research we overcome these problems by giving an optimistic and better technique to hide data without affecting the quality and size of the video. With the help of these techniques the user can hide more than one bit or we can say hide large amount of data in the video, without affecting the quality and size of the video. So it is bang - up and very useful technique Hiding data in video sequences is performed in two main ways: bit stream level and data level. In this paper, we propose a new database block selective embedding type hidden frame that encapsulates Forbidden Zone Data Hiding (FZDH). Through simple rules apply to the frame marker is introduced degree of robustness against drop frame, repetition and insertion attacks.

Scope of the system:

Scope of the system is used in applications are hidden video data for the following advantages: Third person cannot find the original data, It is not easily cracked, To increase the Security, To increase the size of stored data, We can hide more than one bit.

Existing System:

Video data hiding methods is using uncompressed video data. Proposes a high volume transform domain data hiding in MPEG-2 video. QIM apply to low frequency DCT coefficients and adapting the quantization parameter based on MPEG-2 parameters. Furthermore, fouling rate vary depending on the type of the frame. As a result, insertions and deletions occur in the decoder, which causes de-synchronization. They use Repeat Accumulate (RA) codes to withstand scratches. Since adjusting the parameters according to the type of frame, each frame is processed separately. RA codes are being applied to the image data hiding. The results of adaptive block-selection of codes used for synchronization and RA handle deletions. Insertions and deletions can also be handled by convolution codes. The authors use convolution codes embedded. However, the load is placed in the decoder. Multiple parallel Viterbi decoders are used to correct errors of-sync. However, it is noted that this scheme is successful when the number of selected samples of the host signal is much smaller than the total number of received signal samples.

Proposed System:

The new data block based on selective masking frame type embedding forbidden zone that encapsulates data hiding (FZDH) and RA codes according to a further temporal synchronization mechanism. FZDH is a practical method of hidden data, shown to be superior to the conventional quantization index modulation (PCM). RA codes are already used in image and video data hiding due to its resistance against scratches. This robustness allows manipulation of-synchronization between decoder incorporated and which occurs as a result of differences in the coefficients selected.

In order to incorporate frame synchronization markers and which divide the partition into two groups. One group is used for embedding the marker frame and the other bit is used for message. Through simple rules apply to the frame marker is introduced degree of robustness against drop frame, repetition and insertion attacks. Systematic RA codes used to encode message bits and bits of plot marker. Each bit is associated with a block that resides in a group of frames. Random interleaving is performed in space and time, the dependence on local features is reduced.

III. SYSTEM DESIGN

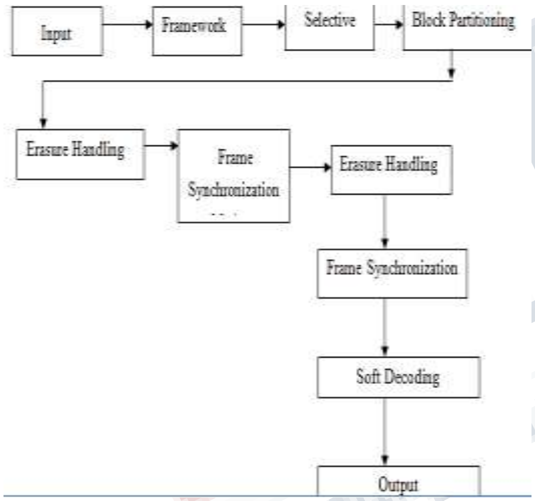

Fig .1: Architecture of the proposed system

3.1 Modules Description

***Input design*: At first, we should need to design to all the process. The design depends up on the process. After finished the design then get the input data's and video. Then precede the following process.

***Framework*: In the first stage, the selection is performed frame and the selected frames are processed block-wise. For each block, only a single bit is hidden. After obtaining 8x8 DCT block, power check is performed on coefficients which are preset in a mask. Variable length selected coefficients are used to hide data bits. Data bit is a message bits member or frame synchronization markers. After the inverse transformation host framework is obtained.

***Selective Embedding*: Host signal samples to be used in data hiding, are determined adaptively. The selection is done in four stages: selection frame, determining frequency band, block selection, and the selection of the coefficients.

***Frame Selection*: Selected number of blocks in the whole frame is counted. If the ratio of selected blocks to all blocks is above a certain value the frame is processed. Otherwise, this frame is skipped.

Frequency Band: Only certain DCT coefficients are utilized. Middle frequency band of DCT Coefficients.

***Block Selection*: Energy of the coefficients in the mask is computed. If the energy of the block is above a certain value then the block is processed. Otherwise, it is skipped.

***Block Partitioning*: Two disjoint sets of data are integrated: message bits and frame synchronization markers. The location of the blocks synchronization marker is determined randomly based on a random key. The remaining blocks are reserved for the bits of message. Partitioning is used the same for all frames. Synchronization markers are embedded frame by frame. Furthermore, the message bits are dispersed consecutive frames. Both results are obtained RA coder.

***Erasure Handling*: As a result of the attacks, or even embed decoder operation can not fully determine the selected blocks embedded in the. To overcome this problem, the error correcting code scratch resistant, such as AR codes are used in image and video data hiding in previous efforts. RA code is a low-complexity turbo-like code. It consists of repetition code, interleave and a convolutional encoder. The code bits are repeated several times R and randomly permuted in accordance with a key.

***Frame Synchronization Markers*: These markers are used to determine frame drops, insertions and repetitions and the final group of time frames in which all the necessary message bits are available for RA decoder. Therefore, it can detect the most likely valid frames. Using the index information of the frame sequence, the robustness is increased. Furthermore, RA spreading code of the code words output from the adjacent frame rates, therefore, errors are less likely to occur when the indices of adjacent frame decoding.

Soft Decoding: A data structure is kept for long channel values observation probability. The structure is initialized with erasures. In each frame, frame synchronization markers are decoded first. Message decoding is performed after the end of the group of frames is detected.

IV. IMPLEMENTATION DESCRIPTION

Firstly we need to take a mpeg compressed video and we need to extract the one image and called as original video frame image as shown in fig 2, and we use a encoder key and the encoder key and the decoder key should be same and using this key we use a random function and generate the encoder image key as shown in fig 3. Now embed the image key as shown in fig 3 in to fig 2 to obtain embedded image as shown in fig 4. Simultaneously we use the same process for decoding the image as shown in the fig 5 and fig 6 to obtain fig 7 the original image.

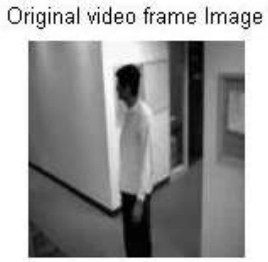

Fig 2: The original image taken from the original video

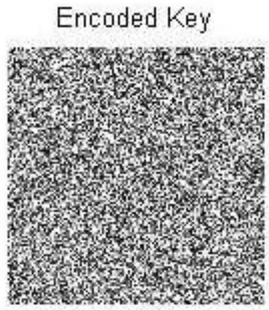

Fig 3: Encoded key

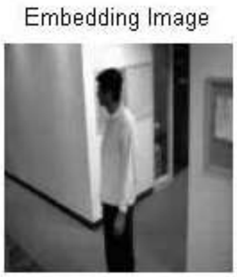

Fig 4: Embedded Image obtained from the original image by using encoded image

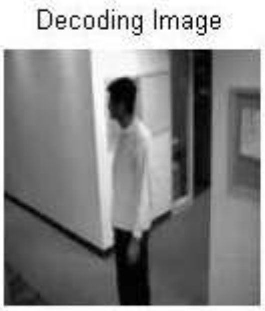

Fig 5: Decoded image obtained by using the key for the encoded image

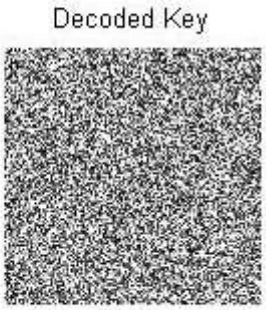

Fig 6: Decoded image key

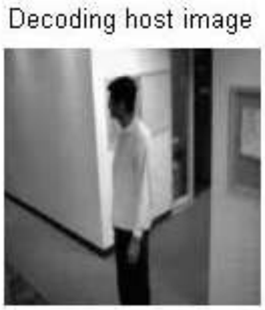

Fig 7: The original image after decoding

V CONCLUSION

In this paper, we proposed a new video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH. The method is also robust to frame manipulation attacks via frame synchronization markers. First, we compared FZDH and QIM as the data hiding method of the proposed framework. We observed that FZDH is superior to QIM, especially for low embedding distortion levels. The framework was tested with MPEG-2, H.264 compression, scaling and frame-rate conversion attacks. Typical system parameters are reported for error-free decoding. The results indicate that the framework can be successfully utilized in video data hiding applications. For instance, Tardos fingerprinting [18], which is a randomized construction of binary fingerprint codes that are optimal against collusion attack, can be employed within the proposed framework with the following settings. The length of the Tardos fingerprint is AC_0^2 In 1/ε1 [19], where A is a function of false positive probability (ε1), false negative probability, and maximum size of colluder coalition, (Co). The minimum segment durations required for Tardos fingerprinting in different operating conditions are given. We also compared the proposed framework against the canonical watermarking method, JAWS, and a more recent quantization based method [2]. The results indicate a significant superiority over JAWS and a comparable performance with [2].

Future Scope:

The experiments also shed light on possible improvements on the proposed method. First, the framework involves a number of thresholds, which are determined manually. The range of these thresholds can be analyzed by using a training set. Then some heuristics can be deduced for proper selection of these threshold values. Additionally, incorporation of human visual system based spatio-temporally adaptation of data hiding method parameters as in [13] remains as a future direction.

REFERENCES

1. S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, “Data hiding in H-264 encoded video sequences,” in *Proc. IEEE 9th Workshop Multimedia Signal Process.*, Oct. 2007, pp. 373–376.

2. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath,“Adaptive MPEG-2 video data hiding scheme,” in *Proc. 9th SPIE Security Steganography Watermarking Multimedia Contents*, 2007, pp.373–376.

3. K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, “Robust image-adaptive data hiding using erasure and error correction,” *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1627–1639,Dec. 2004.

4. M. Schlauweg, D. Profrock, and E. Muller, “Correction of insertions and deletions in selective watermarking,” in *Proc. IEEE Int. Conf. SITIS*, Nov.–Dec. 2008, pp. 277–284.

5. H. Liu, J. Huang, and Y. Q. Shi, “DWT-based video data hiding robust to MPEG compression and frame loss,” *Int. J. Image Graph.*, vol. 5, no. 1, pp. 111–134, Jan. 2005.

6. M. Wu, H. Yu, and B. Liu, “Data hiding in image and video: I. Fundamental issues and solutions,” *IEEE Trans. Image Process.*, vol.12, no. 6, pp. 685–695, Jun. 2003.

7. M. Wu, H. Yu, and B. Liu, “Data hiding in image and video: II. Designs and applications,” *IEEE Trans. Image Process.*, vol. 12, no. 6, pp. 696–705, Jun. 2003.

8. E. Esen and A. A. Alatan, “Forbidden zone data hiding,” in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2006, pp. 1393–1396.

9. B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

10. E. Esen, Z. Do˘gan, T. K. Ates, and A. A. Alatan, “Comparison of quantization index modulation and forbidden zone data hiding for compressed domain video data hiding,” in *Proc. IEEE 17th Signal Process. Commun. Applicat. Conf.*, Apr. 2009, pp. 404–407.

11. D. Divsalar, H. Jin, and R. J. McEliece, “Coding theorems for turbo-like codes,” in *Proc. 36th Allerton Conf. Commun. Control Comput.*, 1998, pp. 201–210.

12. M. M. Mansour, “A turbo-decoding message-passing algorithm for sparse parity-check matrix codes,” *IEEE Trans. Signal Process.*, vol. 54, no.

11, pp. 4376–4392, Nov. 2006.

13. Z. Wei and K. N. Ngan, “Spatio-temporal just noticeable distortion profile for grey scale image/video in DCT domain,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 3, pp. 337–346, Mar. 2009.

14. M. Maes, T. Kalker, J. Haitsma, and G. Depovere, “Exploiting shift invariance to obtain a high payload in digital image watermarking,” in *Proc. IEEE ICMCS*, vol. 1. Jul. 1999, pp. 7–12.

15. T. Kalker, G. Depovere, J. Haitsma, and M. J. Maes, “Video watermarking system for broadcast monitoring,” in *Proc. SPIE Security Watermarking Multimedia Contents Conf.*, vol. 3657. 1999, pp. 103– 112.

16. M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, F. G. Depovere, and J. Haitsma, “Digital watermarking for DVD video copy protection,” *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 47–57, Sep. 2000.

17. K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, “Complete video quality-preserving data hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 10, pp. 1499–1512, Oct. 2009.

18. G. Tardos, “Optimal probabilistic fingerprint codes,” in *Proc. 35th Annu. ACM STOC*, 2003, pp. 116–125.

19. B. Skoric, T. U. Vladimirova, M. Celik, and J. C. Talstra, “Tardos fingerprinting is better than we thought,” *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3663–3676, Aug. 2008.

20. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, “Adaptive MPEG-2 video data hiding scheme,” in *Proc. 9th SPIE Security Steganography Watermarking Multimedia Contents*, 2007, pp. 373–376

21. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett,*Steganography and digital watermarking*” School of Computer Science, TheUniversity of Birmingham. 2003.