International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

VIDEO DATA HIDING IN SELECTIVE PIXELS OF FORBIDDENZONE USING MAPPING FUNCTION

Rejina Basheer [a], Safiya M.K [b]

[a b] *Computer Science and Engineering Department ,Ilahia College of Engineering and Technology,Muvattupuzha,Kerala*'

[a]rejinabshr@gmail.com ,[b]*safiyamoideen@gmail.com*

Abstract

Video data hiding is the process of embedding information into a host medium .Video and audio media are mainly used for data hiding. Data hiding can be secured by using the method of selective embedding and forbidden zone data hiding where blocks are used for data hiding[1] .In this paper video data hiding by selective pixels in blocks is used where the classical LSB concept is adopted, but with the number of LSBs adapting to pixels of different gray levels. A piecewise mapping function according to human visual sensitivity of contrast is used so that the adaptivity can be achieved without extra bits for overhead[2]. Perceptual distortion model, the **just-noticeable-distortion** (JND) ,is applied to improve the subjective quality of compressed videos .The result of selective pixels and LSB concept causes reduction in colour change seen normally in a frame, towards better clarity.The hidden data frame cannot be recognized easily.

***Key words*—LSB,FZDH,JND,DCT**

1.INTRODUCTION

Embedding information in the host medium is the data hiding. Due to the wide presence aural and visual media are used. In this paper we propose a framework for providing security to the information that is hided inside the video image. We use the rail fence encryption technique for the data to providing security to the data .Data hiding in video sequences can be performed in two major ways. That is bit stream level and data level .Data level method are more robust to attacks .However most of the video data hiding method utilize uncompressed video data.

Today Image data embedding has been a popular research issue . It concerns mainly about embedding data into digital media for the purpose of identification, annotation, and message transmission. Applications can often be found in two fields : one is the digital watermarking which provides protection of intellectual property rights and the other is the hiding of secret data within a host or cover signal. Both are constrained with a minimum amount of perceivable degradation to the host signal, which can be an image, audio, or video. In an image there are two zones .That are allowable zone and forbidden zone. In most cases data hiding can be performed in the allowable zone . The data hiding can also be performed on the forbidden zone. Forbidden zone data hiding is the method which depends on the forbidden zone concept, defined as the host signal range where no alteration is allowed during the data process.

In the method of data hiding in single images only less amount of data can be embedded. Whereas by varying the medium to a video, a stream of continuous data can be embedded. The proposed method is used to hide data in a video sequence. Initially the video that acts as the cover media is encrypted. The method then accepts the data that has to be embedded from the user. Post encryption of the data entered, it becomes capable of being embedded into frames, each of which is encrypted. At the receiver side, the data is retrieved and decrypted. The cover media is recovered after data extraction. Since the method is reversible, there must be as little distortions.

Various techniques have been proposed to hide data in images since early times . As known, a video is a sequence of images also called as frames. Hence, the techniques that can be applied in embedding data into an image can also be applied to video streams by applying them to each individual frames. These methods include least significant bit-modifications, masking and filtering, transformations , transform domain embedding and real time video steganography .

Data hiding in video is much way similar to digital watermarking in video. The hidden data must be transparent to a Human Visual System (VHS) and must be imperceptible. It is desirable that the embedding/extraction methods are resistant to attacks. Consecutive frames of a video may look alike. In such cases, new frames that look similar can be inserted into the stream, or new frames can replace

the existing frames . Because each frame carries some hidden data, videos can have an enormous amount of data embedded. Data hiding has been used in various applications like copyright protection, authentication, fingerprinting, error concealment, broadcast monitoring, covert communication, etc. Each application imposes different types of constraints in terms of capacity, security and robustness. Privacy is protected by obfuscating images of individuals from the video and the original data is preserved by hiding it in the compressed bit stream of the modified video. This is particularly useful when a condition arises to prove the authenticity of the modified video. In general, visual and aual 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 media type. The transmission of video signals over noisy wireless channels may cause inevitable errors that might severely degrade the visual message.

In wireless communication systems, in order to handle such errors, some error concealment techniques have been proposed in three major groups. These techniques try to recover the lost data either by an interaction between the encoder and decoder, as a re-send signal, or post-processing operations at the decoder to recover lost information, or leaving some extra redundancy at the encoder to minimize the reconstruction error.

2.RELATED WORKS

Several solutions were proposed to hiding the data in a video .But the security of the data is important. In paper[1] a method proposed is that security can be provided to the data by using an encryption technique .In [1] the encryption technique which is used is rail fence technique . A block based adaptive video data hiding that incorporates FZDH(Forbidden zone datahiding) .In this paper we use selective embedding to determine the host signal samples. The selection performed in four stages .The four stages are framework ,selective embedding , block partitioning and erasure handling .In this hiding technique we use rail fence algorithm for providing security to the data. Selective embedding is the technique to determine the host signal samples for data hiding .Forbidden zone concept is defined as the area in which no alteration is possible.

Then the average energy of the block is expected to be greater than a predetermined threshold. In the final stage, the energy of each coefficient is compared against another threshold. The unselected blocks are labeled as erasures and they are not processed. For each selected block, there exists variable number of coefficients. These coefficients are used to embed and decode single message bit by employing multidimensional form of FZDH that uses cubic lattice as its base quantizer.

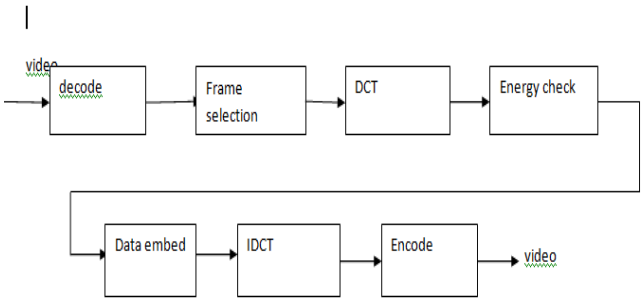


Fig 1.Embedder Flowchart of the proposed video data hiding framework for a single frame

In [2] wavelet-based embedded bit plane coding techniques are used for rate scalable coding. Further, we exploit the foveation feature of the HVS, which refers to the fact that the HVS is a highly space-variant system, where the spatial resolution is highest at the point of fixation (foveation point) and decreases dramatically with increasing eccentricity.

By taking advantage of this fact, considerable high frequency information redundancy can be removed from the peripheral regions without significant loss in the reconstructed image and video quality.. If attention is focused at the foveated region, then the foveated and the original images have almost identical appearance (depending on the viewing distance). The foveation factor has been employ fixed in previous work to improve image and video coding efficiency. However, most of the algorithms used fixed foveation models. These methods lack the flexibility to adapt to different foveation depths and are not convenient to be implemented in a rate scalable manner not considered in depth, and no efficient coding algorithms were implemented.

Most data hiding schemes use uncompressed video data. Compression of the video may bring forth certain errors in the stream, which are marked using repeat accumulate (RA) codes. A block – based selective embedding type data hiding encapsulates forbidden zone data hiding (FZDH) [3] and RA codes [6] with an additional temporal synchronization mechanism. Here, each block is partitioned into two groups. One group is used for frame marker embedding and the other is used for message bits. By means of simple rules applied to the frame markers, certain level of robustness against frame drop, repeat and insert attacks are brought in. This method is used for both MPEG-2 and H.264 videos.

Segmenting the frames into blocks before data embedding is not a new concept. The H.264 video encoder uses various block sizes during inter prediction as opposed to a fixed size used in the present paper. Using this property of varying block sizes, desirable data can be hidden and extracted without knowledge of the original video content [4]. Based on the size of the block or the block type in the

frame, a binary number is assigned to each of the blocks. The message to be embedded is also converted to binary bits and two of them are paired. This method then hides the bit pair in blocks, either consecutively or in a predefined pattern.

In paper[5] designing visual communication systems is to use the least resources to achieve the highest visual quality with respect to certain constraints such as bit rate, complexity, and maximum delay. In most circumstances, the human visual system (HVS) makes final evaluations on the quality of images and video that are processed, transmitted, and displayed. Thus, it is essentially futile to spend significant effort on encoding those signals that are beyond the human perception. Just noticeable distortion (JND), which accounts for the maximum distortion that the HVS does not perceive, can serve as a perceptual threshold to guide an image/video processing task.

In image compression schemes, JND can be used to optimize the quantizer or to facilitate the rate-distortion control . Information of higher perceptual significance is given more bits and preferentially encoded, so that the resultant image is more appealing In video compression schemes, JND plays more diverse roles. In this paper, we propose a method for explicit JND estimation in the DCT domain, with integrated formulation for both images and video. The model incorporates spatio-temporal CSF, eyemovements, luminance adaptation, and intra- and inter-band contrast masking.

The use of formulas in hiding data into the frame creates a higher level of complexity. Thus it strengthens the algorithm. Methods like Entropy Thresholding Scheme [7] or Selectively Embedding in Coefficients Scheme use various formulas in data hiding. These methods, applied to images can easily be extended to videos. Entropy Thresholding Scheme divides a frame into a number of non-overlapping blocks. A discrete cosine transform of these blocks are taken. Energy of these blocks is then calculated based on some formulas. Blocks that have energy below the threshold energy are only used for data hiding. In Selective Coefficients method, the frame is partitioned into a number of zones. Some of the zones are forbidden from hiding any data into them while the others are chosen for embedding.

3.PROBLEM DOMAIN

The rapid growth in the demand and consumption of the digital multimedia content in the past decade has led to some valid concerns over issues such as content security, authenticity, and digital rights management. Multimedia data hiding, defined as imperceptible embedding of information into a multimedia host, provides potential solutions, but with many technological challenges.

Ever improving network bandwidths, computer speeds, digital storage capacities, and wireless capabilities are changing our lives right from the way we entertain ourselves, communicate with each other, or assimilate and disseminate knowledge, to the way we operate our bank accounts. A key driver for these changes has been the rapid growth in the demand and consumption of digital multimedia content. This has, however, lead to some valid concerns over multimedia content security, authenticity, and intellectual property rights. Because of its potential applications in multimedia content security, data hiding or data embedding continues to receive considerable attention from the research community.

Text documents are omnipresent everyday: newspapers, books, web pages, contracts, advertisements, checks, identification documents, etc. Data can be hidden among these texts too in some predefined pattern. An audio watermark is a kind of digital watermark —a marker embedded in an audio signal, typically to identify ownership of copyright for that audio. Watermarking is the process of embedding information into a signal (e.g. audio, video or pictures) in a way that is difficult to remove. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time. Watermarking has become increasingly important to enable copyright protection and ownership verification

A few fundamental issues of data hiding in image and video. We have proposed general solutions, including how to embed multiple bits, how to handle uneven embedding capacity, and how to allow the number of reliably extractable bits to be adaptable to the actual noise condition. apply the solutions to specific design problems and present details of embedding data in image and video. Embed data in images at two levels, each of which is designed for different robustness.

This approach allows for graceful decaying of extractable information as noise gets stronger. In Section III, we extend the multilevel embedding to video, for which difficulty arises because the embedding capacity varies from region to region within a frame as well asfrom frame to frame. We embed control information to facilitate the extraction of the user data payload and to combat such distortions as frame jitter.

Data hiding has been used in various applications like copyright protection, authentication, fingerprinting, error concealment, broadcast monitoring, covert communication, etc. Each application imposes different types of constraints in terms of capacity, security and robustness. Privacy is protected by obfuscating images of individuals from the video and the original data is preserved by hiding

ISSN:2319-7900

it in the compressed bit stream of the modified video. This is particularly useful when a condition arises to prove the authenticity of the modified video. In general, visual and aural media are preferred due to their w ide presence and the tolerance of human perceptual systems involved. Although the general structure of data hiding process does not depend on the media type. The transmission of video signals over noisy wireless channels may cause inevitable errors that might severely degrade the visual message. In wireless communication systems, in order to handle such errors, some error concealment techniques have been proposed in three major groups. These techniques try to recover the lost data either by an interaction between the encoder and decoder, as a re-send signal, or post-processing operations at the decoder to recover lost information, or leaving some extra redundancy at the encoder to minimize the reconstruction error

.Data hiding in video sequences is performed in two major ways: bit stream-level and data-level. In bit stream-level, the redundancies within the current compression standards are exploited. Typically, encoders have various options during encoding and this freedom of selection is suitable for manipulation with the aim of data hiding. However, these methods highly rely on the structure of the bit stream; hence, they are quite fragile, in the sense that in many cases they cannot survive any format conversion or transcoding, even without any significant loss of perceptual quality. As a result, this type of data hiding methods is generally proposed for fragile applications, such as authentication. On the other hand, data level methods are more robust to attacks. Therefore, they are suitable for a broader range of applications.

5.PROBLEM IDENTIFICATION

.Video and audio media are mainly used for data hiding. Data hiding can be secured by using the method of selective embedding and forbidden zone data hiding where blocks are used for data hiding the blocks constitute a set of image frames in forbidden zone based on selective embedding technique.[1] Where the video is divided into frames and the data is hidden into selected frames , such frames are seem to be easily recognizable by the human due to the presence of color change. Better security to the data can be provided by using selective pixel embedding and rail fence technique[2].

There are three main conflicting requirements of a multimedia data embedding system: perceptual transparency, robustness, and capacity. Information embedding into a multimedia host should not incur any perceptual distortion to the host, i.e., the composite signal should be perceptually transparent. The data should be recoverable even after the composite multimedia signal has undergone a variety of attacks, intentional or unintentional, to remove the embedded data. In other words, the hidden data must be robust against a variety of attacks.

We would also like to embed as many bits into the host as possible, or, the capacity of the embedding system should be high. 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. For instance, image and video data hiding share many common points; however video data hiding necessitates more complex designs as a result of the additional temporal dimension. Therefore, video data hiding continues to constitute an active research area.

Data embedding or data hiding can be done on audio, video and textual files.In this paper Data embedding is done in a video file owing to the data's confidential value. It thus is important to keep the embedded data secure. Also, it must not be extracted by any third party attacks. The security of the system is compromised when a third party gains access to the data.

5.1 advantages of selective pixels in forbidden zone

- Probability of detection is less
- only selective pixels are consider for hiding the data

.

6. PROBLEM DEFINITION

The video data hiding can be done by using forbidden zone concept[1].The disadvantage is that the frame with hidden data can be recognised easily by seeing the distorted frame.The Video data hiding in selective pixels select selective pixels using mapping function[2]

7.PROBLEM STATEMENT

In this paper the data hiding is done in the selective pixels located in forbiddenzone using a mapping function.It is the integration of the concepts of references [1] and [2]

4.1 example:

Suppose a sender A want to send a secret data to the reciever B the sender may have the following requirements:

- the data should be confidential

ISSN:2319-7900

- the data hiding image cannot be recognized

The normal procedure as follows:

- select the image
- hide the data

Consider a situation when A sends a video file,where efficient hiding scheme needs to be proposed. Larger amounts of data can be hidden to the video file by A. In the proposed paper, embedding data in the video file proceeds as follows:

- divide the video to frames
- input numeric and textual data for hiding
- hide the data within the selective pixels of the forbidden zone of image using mapping function
- Encrypt the data using rail fence technique.

8 .PROPOSED SYSTEM

In this paper, we propose a new method to embed a series of secret data into a host image. The secret data is assumed to be in a form of binary bit streams, which can be raw or compressed multimedia, or simply a series of texts conveying messages for transmission. The classical LSB concept is adopted, but with the number of LSBs adapting to pixels of different gray levels. A piecewise mapping function according to human visual sensitivity of contrast is used so that adaptivity can be achieved without extra bits for overhead. Perceptual distortion model the **just-noticeable-distortion** (JND) is applied to improve the subjective quality of compressed videos.Our method is based on the human visual system in such a way that gray value change of each pixel in the host image after embedding is beyond human perception. Also, the embedded secret data can be extracted without the knowledge of the original host image.

8.1.Framework

The proposed system uses a method embedded multimedia data into a host image .In this paper we use the text as the multimedia data. The embedding operation for a single frame is Y-channel is utilized for data embedding. In the firststep, frame selection is performed and the selected frames are processed block-wise. For each block, only a single bit is hidden. After obtaining 8 × 8 DCT of the block, energy check is performed on the coefficients that are predefined in a mask. Selected coefficients of variable length are used to hide data bit *m*. *m* is a member of message bits or frame synchronization markers. Message sequence of each group is obtained by using RA codes for *T* consecutive frames. Each block is assigned to one of these groups at the beginning. After the inverse transform host frame is obtained. The classical LSB concept is used but with number of LSB's adapting to pixels of different gray levels. A piecewise mapping function according to human visual sensitivity of contrast is used so that adaptivity can be achieved without extra bits for overhead.

Traditional LSB method hides data in a fixed number of LSB's in a an image pixel .In this we use an LSB mapping function which gives the number of LSB's that can be used for each possible gray level g is to be devised. Decoder is the dual of the embedder, with the exception that frame selection is not performed. Fig. 3 shows the flowchart for a single frame. Marked frames are detected by using frame synchronization markers. Decoder employs the same system parameters and determines the marked signal values that will be fed to data extraction step. Non-selected blocks are handled as erasures. Erasures and decoded message data probabilities (*om*) are passed to RA decoder for *T* consecutive frames as a whole and then the hidden data is decoded.

8.2.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.

1) 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 (*T*0) the frame is processed. Otherwise, this frame is skipped.

2) Frequency band: only certain DCT coefficients are utilized.
Middle frequency band of DCT coefficients.

3) Block selection: energy of the coefficients in the mask

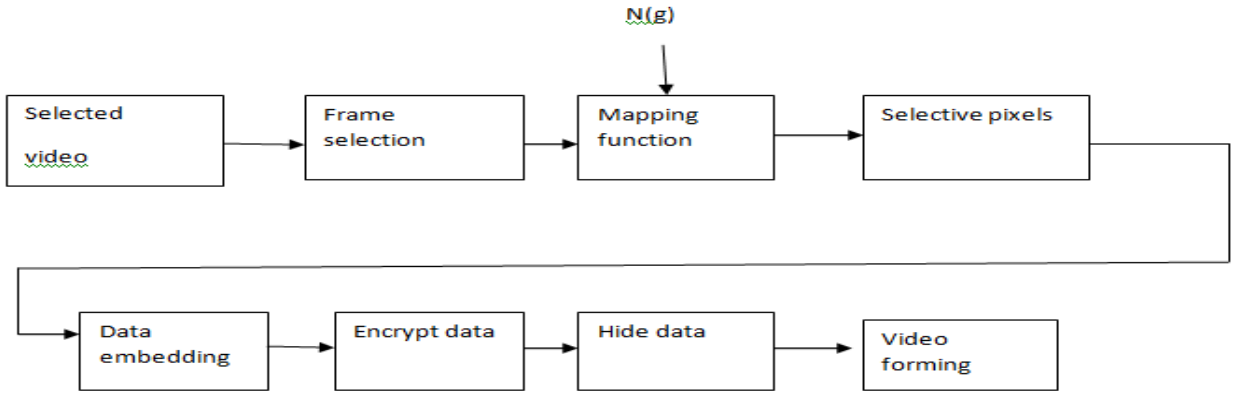


Fig 2:data hiding process in the embedder

is computed. If the energy of the block is above a certainvalue (*T*1) then the block is processed. Otherwise, it is skipped.

4) Coefficient selection: energy of each coefficient is compared to another threshold *T*2. If the energy is above
*T*2, then it is used during data embedding together with
other selected coefficients in the same block.

Mapping function

Traditional LSB method hides data in a fixed number of **LSBs** of an image pixel. The more the **LSBs** are changed, the more distortion we get. Actually, the number of LSBs for data embedding is pixel-dependent according to the above discussion and we should adaptively modi@ gray levels within different tolerances of human visual system's sensitivity to contrast variation.

Hence an LSB-mapping function ***N(g)*** , which gives the number of LSBs that can be embedded for each possible graylevel g, is to be devised. Let the pixel value after embedding be denoted by g' , then the condition of no overhead for this adaptation is that the N(g)values before and after pixel modification should remain unchanged, i.e., N(g') = ***N (g).*** the gray level difference |g'-g| should be subject to constraint of C(g).N(g) is made piecewise step as per the following formula[2].The tabular form of data by using the above equation is shown as below[2].

$$N(g)=\begin{cases}1 & 0\le g<k_1\\ 2 & k_1\le g<k_2\\ 3 & k_2\le g<k_3\\ 4 & k_3\le g<256\end{cases}$$

Table 1. Statistics of $C(g)$ and $N(g)$ over the entire range of graylevels.

g	0-30	31-48	49-69	70-85	86-97	98-109
$C(g)$	3	4	5	6	7	8
$N(g)$	2	2	2	2	3	3

g	110-121	122-134	135-146	147-158	159-170
$C(g)$	9	10	11	12	13
$N(g)$	3	3	3	3	3

g	171-182	183-195	196-207	208-219	220-230
$C(g)$	14	15	16	17	18
$N(g)$	3	4	4	4	4

g	231-236	237-242	243-248	249-253	254-255
$C(g)$	19	20	21	22	23
$N(g)$	4	4	4	4	4

8.3.Block Partitioning

ISSN:2319-7900

Two disjoint data sets are embedded: message bits ($m1$) and frame synchronization markers ($m2$). The block locations of $m2$ are determined randomly depending on a random key. The rest of the blocks are reserved for $m1$. The same partitioning is used for all frames. $m2$ is embedded frame by frame. On the other hand, $m1$ is dispersed to T consecutive frames. Both of them are obtained as the outcomes of the RA encoder[1]

8.4.Erasure Handling

Due to adaptive block selection, de-synchronization occurs between embedder and decoder. As a result of attacks or even embedding operation decoder may not perfectly determine the selected blocks at the embedder.RA codes are used to overcome this problems. RA code is a low complexity turbo-like code . It is composed of repetition code, interleaver, and a convolutional encoder. The source bits (u) are repeated R times and randomly permuted depending on a key. The interleaved sequence is passed through a convolutional encoder with a transfer function $1/(1 + D)$, where D represents a first-order delay[1].

8.5.Frame Synchronization Markers

Frame synchronization is the process of synchronizing display pixel scanning to a synchronization source. When several systems are connected, a sync signal is fed from a master system to the other systems in the network, and the displays are synchronized with each other.While receiving a stream of framed data, **frame synchronization** or **framing** is the process by which incoming frame alignment signals (i.e., a distinctive bit sequences or syncwords), are identified (that is, distinguished from data bits), permitting the data bits within the frame to be extracted for decoding or retransmission.

Each frame within a group of T consecutive frames is assigned a local frame index starting from 0 to $T - 1$. These markers are used to determine the frame drops, inserts and repeats, as well as the end of the group of frames at which point all necessary message bits are available for RA decoder[1].

8.6.Soft Decoding

At the decoder, a data structure of length $RK1$ is kept for channel observation probability values, om. The structure is initialized with erasures ($om = 0.5$ for $m = 0$ and $m = 1$). At each frame, frame synchronization markers are decoded first. Message decoding is performed once the end of the group of frames is detected.Two frame index values are stored: current and previous indices. Let $f$cur and $f$pre denote the current and previous frame indices, respectively. Then the following rules are used to decode $u1$.

1) If $f$cur > T, then skip this frame. (This case corresponds to unmarked frame.)

2) If $f$cur = $f$pre, then skip this frame. (This case corresponds to frame repeat.)

3) Otherwise, process the current frame. Put om values in the corresponding place of the data structure. Nonselected blocks are left as erasures.If $f$cur< $f$pre, then the end of the group of frames is reached. Decode the message bits and obtain $u1$. Initialize data structure[1].

In this proposed system there are 2 section that are encoding section and decoding section .In encoding section initially the video is divided into frames. That is image formation is performed. The next step is that input the data which is to be hidden. The data is hided into the last image of the video. The data is hided according to the lsb concept .The data is hided in to the selected pixels of the image .For providing better security to the data we use rail fence encryption technique. After that the video is formed. Decoding the data is the second section. In the decoding stage the data is retrieved at the receiver side.

The encoding part of video data hiding process consist of 5 steps.

1 . Selecting the video

The encoding process starts with selecting the videos select the video that is used for data hiding. Video can be selected from any location of the computer. This video is divided into frames in the next step.

2. Image formation

The cover media, here the video, is initially divided into multiple frames. Each of these frames is an image. The frame is encrypted using any one of the convenient encryption mechanisms with a frame key. The frame key is symmetric. That it, the sender and receiver uses the same key in encryption and decryption of the frame. After the data to be embedded is accepted from the user, it is encrypted using a data key. The encrypted data in binary is embedded into the frame This data is then decrypted using the same data key. The data are then collected to form a string that is the same data that was embedded from the sender.In this step images of the

ISSN:2319-7900

above video is created. Each image is created with a 0.2 nanoseconds.

3. Input data

Input the data which is to be hided in to an image .In this paper we use the multimedia data is text .The text may be either numerical , alphabets or combination of both. The data which is given as input is converted into its corresponding binary form.

4. Hide data

Data is hided into an image according to certain criteria .In this paper we use the classical lsb concept with the help of human visual perception .The pixels which will be used for hiding the data is selected by using a piecewise mapping function. LSB-mapping function ***N(g)*** , which gives the number of LSBs that can be embedded for each possible graylevel g .

5. Video forming

The video is formed with data hided image in addition to the other images. This video consist of the secret data which will be send to the reciever

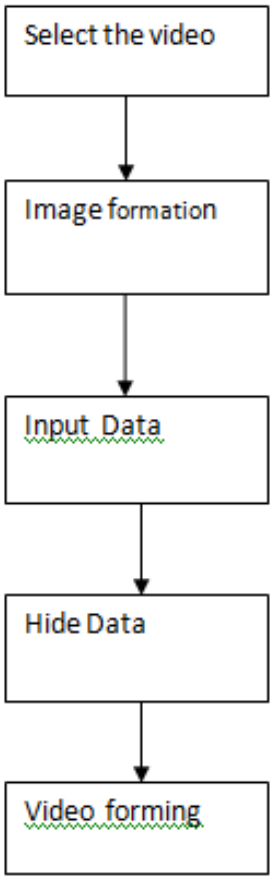


Fig 3:steps in encoding process

The decoding part of the video data hiding process consist of 2 steps

Steps in decoding process

1 .Select the folder

Select the folder for which the data to be retrieved.That is browse the location of the folder to which data to be stored.

2 .Data Retrieval

In the data hiding process the data hiding into the selected image .The image is selected according to classical lsb concept. The data which is hidden in the image is retrieved in this.

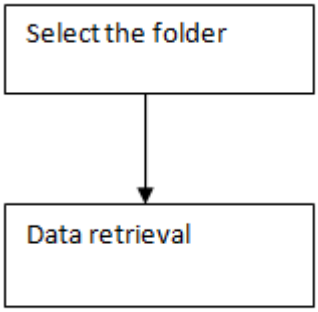


Fig 4.steps in decoding process

From the above two figures we can see that the the encoding consist of 3 steps. And decoding consist of 2 steps.The additional operation we are done on selecting the pixels for which the data is hiding is the mapping function.By using the mapping function we can decide the number of lsb used for data hiding depending on the grey level values

9. SIMULATION

The proposed work has been implemented in java. Java is a general purpose, concurrent, class-based, object oriented programming language that is intended as “write once, run anywhere”. Java has many packages that helps in its successful running. The image processing parts of Java are buried within java.awt.image package. One characteristic of Java is portability, which means that computer programs written in the Java language must run similarly on any hardware/operating-system platform. This is achieved by compiling the Java language code to an intermediate representation called Java bytecode, instead of directly to platform-specific machine code. Java bytecode instructions are analogous to machine code, but they are intended to be interpreted by a virtual machine (VM) written specifically for the host hardware. End-users commonly use a Java Runtime Environment (JRE) installed on their own

ISSN:2319-7900

machine for standalone Java applications, or in a Web browser for Java applets.

Standardized libraries provide a generic way to access host-specific features such as graphics, threading, nd networking.A major benefit of using bytecode is porting. However, the overhead of interpretation means that interpreted programs almost always run more slowly than programs compiled to native executables would. Just-in-Time (JIT) compilers were introduced from an early stage that compile bytecodes to machine code during runtime.

Apart from Java, particular softwares are also used in conversion of video to frames. Various software are available in the market that provide for this conversion like XVideoConverter, DVDVideoSoft, Ffmpeg etc. These software are capable of editing and converting audio and video files between different formats. It can sample 10, 30, 50, 100, 500, or 1,000 frames, in intervals of 1, 2, 5, 10, and 20 seconds, making multiple screenshots. Various other features are also available in these software that enables you to trim the video and select a fragment to capture or that makes 3D pictures and videos.

The model has been simulated in a Linux environment under the Java taking aid of the Ffmpeg software. Ffmpeg is a multimedia framework able to decode, encode, transcode, mux, demux, stream, filter and play most formats. It is easy to use, fast, light and saves time. It can easily convert video to audio or images.

Ffmpeg is a software that produces libraraies and programs for handling multimedia data.It includes libavcodec an audio or video codec libraray used by several other projects,libavformat,an audio or video ontainer mux and demux libraray, and the ffmpeg command line program for transcoding multimedia files.the software sequence model of the proposed work is depicted. The video stream that acts as the cover media is sent to Ffmpeg software. Sequences of frames are created in this process. These frames are then input to the project, run in Java. Java code encodes each frame using the frame_encode() function.

INPUT
OUTPUMODEL

Sl no:	INPUT	PROCESS	SIMULATION CODE	OUTPUT	REMARKS
1	Select thevideo	Convert into frames	ffmpeg()	Sequence of frames	
2	Sequence of RGB frames	Ycbcr conversion	get RGB_YCC()	Sequence of ycbcr frames	
3	Input the data	Input data is converted to binary form	bit conversion()	Binary form of data	Data may be textual or numeric
4	Hide data	Using encryption technique	encode text()	Data encrypted	Technique used is railfence
5	Video forming	Sequence of frames are combined	ffmpeg()	Video formed	
6	Select the folder	Data decryption	decode text()	Data retrieved	

10.RESULT AND ANALYSIS

A comparative study between thee datahiding schemes are discussed below.From the below table we can understand that the data hiding technique which uses mapping function is more secure.In FZDH and classical lsb concept datahiding is done but the security is not provided.In the third scheme that is the data hiding method which uses a mapping function for selecting the pixels.For providing better security
to the data an additional encryption technique is also used.

Datahiding method	encryption technique	security	chance of hacking
FZDH	nil	less	more
Classical lsb concept	nil	less	less
Using mapping function	yes	high	less

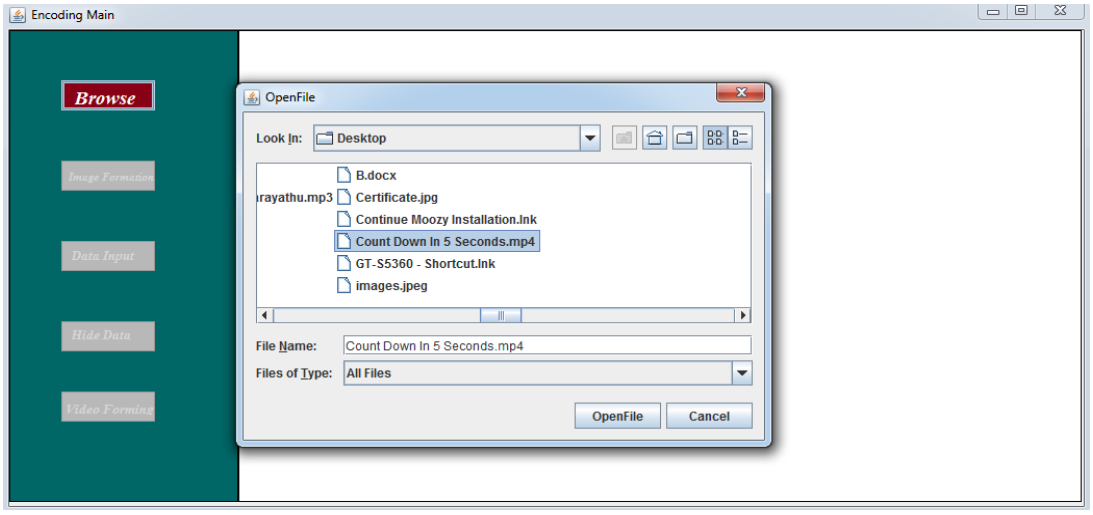
ISSN:2319-7900

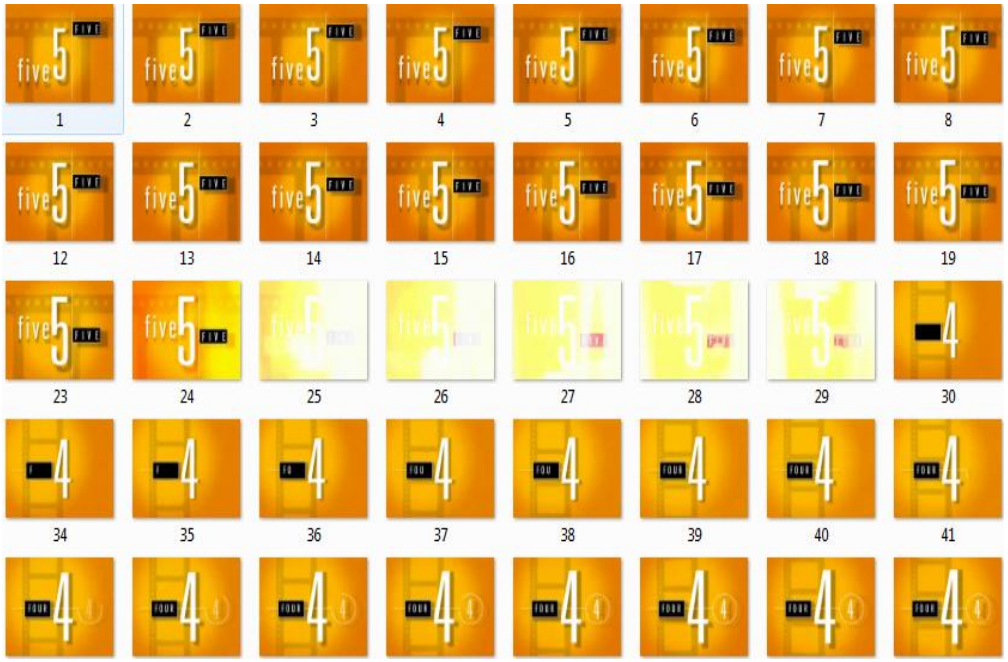
The video data hiding method process starts with this.

:

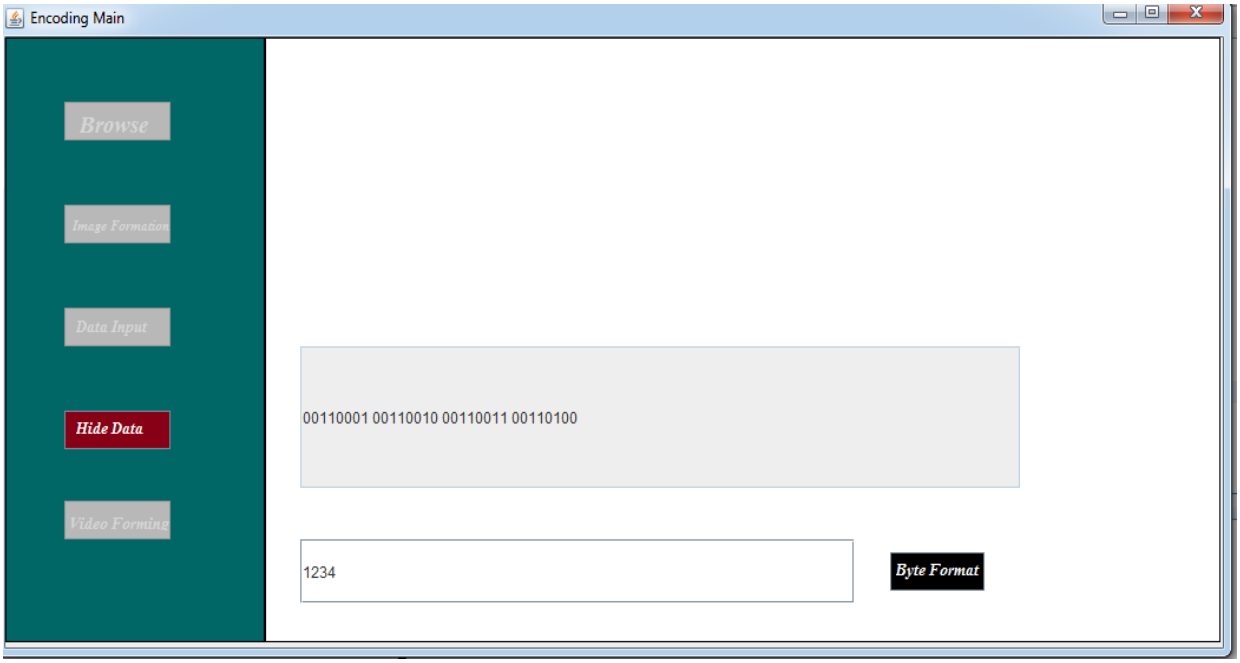
ISSN:2319-7900

When the user login to the page using the username and password the above window appears.From this window we can browse the video which can be used for datahiding.The next step is image formation.The video can be divided into images.



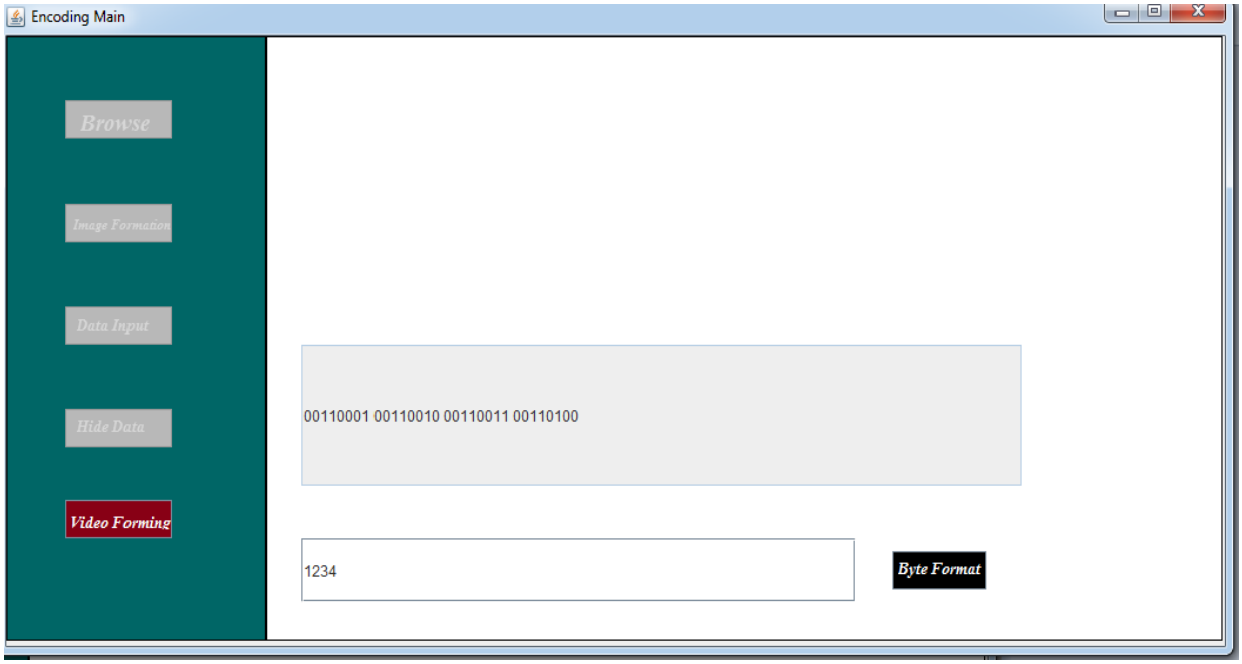


The above picture is the images which can be formed by this video.The next step is hiding the data in the image. This can be of alphabet or numeric form.This input can be converted to its corresponding ASCII value and then it is again converted to its binary value.



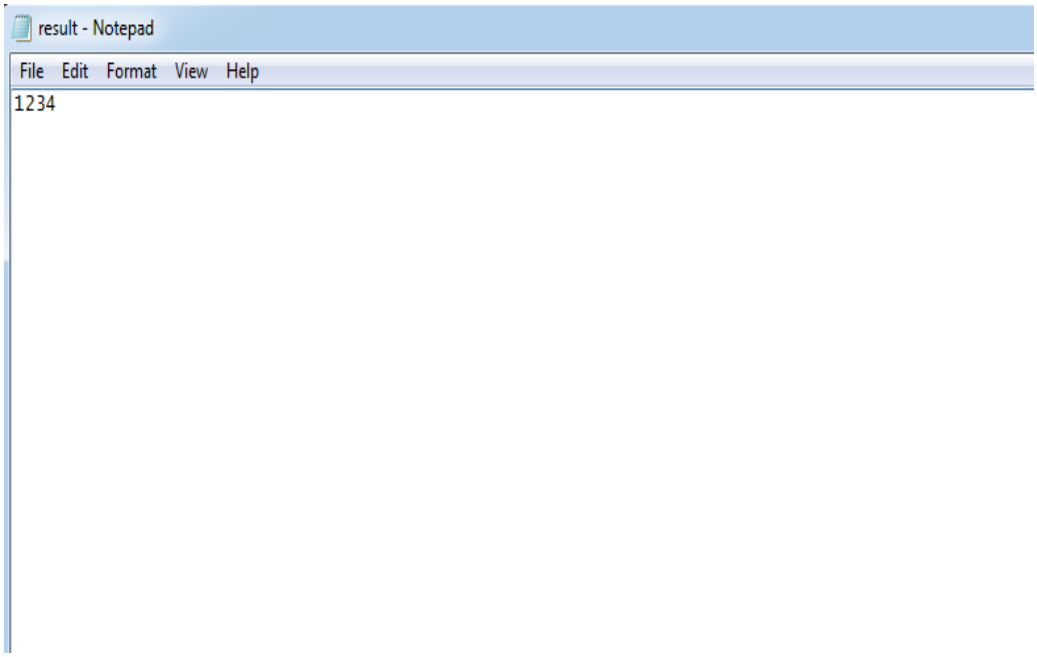
Input the data which is to be hide inside the image,This can be of alphabet or numeric form.This input can be converted to its corresponding ASCII value aand it again converted to its binary form.

ISSN:2319-7900



The last stage in the encoding process is video forming.That is the image with data hide also combined with other image and the video is formed.

This window indicates that the video is successfully formed.



Retrieve the data which is hide inside the image.

CONCLUSION

A video data hiding approach in which the host signal which can be used for data hiding is selected by selective embedding and forbidden zone concept. In addition to this we use the properties of human visual system. A piecewise mapping function according to human visual sensitivity of contrast is used so that adaptivity can be achieved without extra bits for overhead. In this paper we use the classical lsb concept for selecting the pixels .Video data hiding in human visual system is an approach to hide the date in a video in a secure way by using the concepts in human visual system.

ACKNOWLEDGMENT

The authors wish to thank the CSE department for their support and help in completing this work.

REFERENCES

[1] E. Esen and A. A. Alatan, ―Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding‖, in IEEE transactions on Circuits and Systems for Video Technology, vol.21, NO. 8, Aug 2011

[2] 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

.[3] E. Esen and A. A. Alatan, "Forbidden zone data hiding," in Proc. IEEEInt. Conf. Image Process., Oct. 2006, pp. 1393–1396.

[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] 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.

[6] G. Tardos, "Optimal probabilistic fingerprint codes," in 35th Annu.ACM STOC, 2003, pp. 116–125

[7] A. 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

[8] Da-Chun Wu and Wen-Hsiang Tsai, "Image Hiding inSpatial Domain Using An Image DifferencingApproach," Proc. Of 1998 Workshop on Computer Vision, Graphic

ISSN:2319-7900