ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 30-35 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

A Novel Approach for Detection and Prevention of Online Video Piracy

Gummaluri Sai Kumar[1],Gudipudi Manikanta[2]
[1]MVGR College of Engineering, India, saikumargummaluri@gmail.com
[2]MVGR College of Engineering, India, manikanta.gudipudi539@gmail.com

Abstract—Copyright Infringement is the burning problem from the past decade. This violation of copyrights is not limited to a single area alone but has covered a wide spectrum. Piracy of Videos is the most important amongst all. Video is the most informative and effective means of communication. Further, a video stands as an example of intellectual thinking of the one who builds it and can serve as a mean of economy. Illegally replicating the video content is causing huge damage economically and intellectually. In this paper, we are proposing a framework that makes use of LSB to prevent the illegal uploading and downloading of authorized video content. The obtained results are also supporting the fact that this technique can effectively be used to judge the authenticity of the video that is being uploaded or downloaded and helps to protect the copyrights of the individuals.

***Keywords*:**Video Piracy, Copyright Infringement, LSB, Haar Cascades.

INTRODUCTION

Movie is the most prevalent part of media. Be it a commercial movie or a non-business one, it has hurled its follow on each way of human action. They have come to be so much mainstream in light of the fact that they are the most widely used medium for information trade and used for various purposes. Other generally critical and intriguing angle is that there is no particular age or gender group who favor motion pictures. Further, they might be of huge monetary value moreover. Movies specifically, are the essential substances which furnish immense profits to both people who own it and to those who rely on upon it. In spite of all this, the face of movie in multimedia is varying due to the illegitimate actions of individuals.

Though people think of piracy as a case of only videos, this has its roots in various other elements of multimedia and information technology as well. The latest growth in the technology further ignited this rampant misuse. One best example of this scenario is the loss that is incurred by the Motion Pictures Association America (MPAA). It summed up to a whopping amount of $250 billion and is still growing every year. In view of this scenario, many legal steps like implementing laws against the illegal reproduction and usage of intellectual content in the form of videos have been taken. But nothing could provide a substantial solution to the problem.

The statistics stating that around 22% of the bandwidth globally is used for online piracy [17] brings out the seriousness of the problem. Also, majority of the content that is transferred over the P2P networks is copyrighted. In order to handle the scenario, we in this paper, attempt to provide an approach which can help to detect and prevent the unauthorized uploading of videos onto the web. This is done by taking into account the various factors that are responsible for the dynamic nature of the videos. The rest of the paper deals with the technique in detail.

LITERATURE REVIEW

Data Hiding is a technique which has its roots back to the 14th century. Several techniques have been developed for the purpose of achieving secrecy for the information distribution. One such technique is the Least Significant Bit (LSB) Algorithm [1],[8]. In this, the information that is needed to be transferred is embedded at the bit level by choosing some particular pixel. But the choice of the pixel for embedding is always critical.

Many modified versions of this LSB have been developed. Discrete Cosine Transformation (DCT)[16] is one such approach. Ying Wang et. al.[10] proposed one such method for steganography based on DCT. EktaWalia*et al.*[7] also put forward a technique based on DCT. Both these approaches use DCT in order to choose a pixel into which the data is embedded.

In order to provide additional security to the data, Mazen Abu Zaher[5] proposed the technique of Modified LSB wherein the data that is to be embedded is encrypted prior to embedding. Gabriel MachariaKamau*et al.*[2] proposed an enhanced LSB Steganographic method standard minimal Liner Congruential number Generator (LCG) for the purpose of choosing the image bits for insertion. This results in the improvement of imperceptibility of the message that is hidden. Apart from this, VajihehSabeti*et al.*[3] developed another technique which uses Octonory Complexity Measure.

Coming to the face detection, the first potential framework is developed by Paul Viola and Michael Jones [9]. They have developed the Haar-Like features which can effectively be used for detecting of faces. Prior to this, a general frame work for object detection is given by Constantine P. Papageorgiou*et al.*[14]. They have developed a technique for object detection

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 30-35 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

in static images from cluttered scenes. Rainer Lienhart and JochenMaydt[12] developed an extended set of Haar-Like features for Rapid Object Detection. In this, they have introduced a set of rotated haar-like features which enhanced the performance when compared to the traditional haar-like features.

METHODOLOGY

Two major steps form the core of the entire approach. The first part deals with extraction of the features from the video, which form the feature library and the second part deals with embedding the secret message into the video that is being analyzed. The following gives the explanation of each of the steps in detail.

Building the Feature Set

The entire process begins with this step. Here, the features that form the part of the feature set are the faces that occur and the time of occurrence of each of the face and their individual frequency counts.

For the purpose of detecting and extracting faces from the video, we use the Haar-Cascades. Viola-Jones first developed the Haar-like features, which evolved to be the framework for visual detection. We choose multiple haar-like features like eyes, nose, face and mouth for achieving better results.

As a part of the framework developed by Viola-Jones for visual detection, we have the concept of rectangular features. All the above mentioned features come under the category of rectangular features. Integral Images are used to compute these rectangular features (Fig 1). The Integral Images are computed as shown in Fig 2.

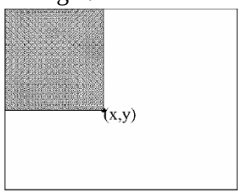

Fig1: Computing the value of integral image at a point (x,y).

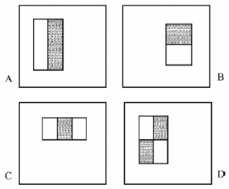

Fig2: Haar-like feature set

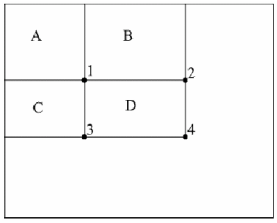

Fig3: Sum of Pixels at position D is given by 4+1-(2+3)

Further, the decision of whether a search window contains a face or not, is made based on the Adaboost [15] strong classifier. If the frame contains a face, then H(x)=1 and is 0 if otherwise.

$$H(x) = \begin{cases} 1 \; if \sum_{i=1}^{T} \propto h_i(x) \geq \emptyset \\ 0 \; otherwise \end{cases} \quad (1)$$

$$h_j(x) = \begin{cases} 1 \; if \; p_j f_j(x) < p_j \theta_j \\ 0 \; otherwise \end{cases} \quad (2)$$

In order to balance any disturbances in the intensities that might have occurred, the features (faces) that we extract are subjected to Histogram Equalization [13] before being added to the feature set. Also, the algorithms that are used in the entire process are presented below.

Input: Video ' V' that is composed of 'N' number of frames i.e., V= { f_1, f_2, f_3,…… f_N}
Output: Feature Set that represents the features of the video
$I_f \leftarrow$ frame selection interval
1.foreach $k \leq N - I_f$ **do**
2. $k = k + I_f$
3.Extractfeatures(f_k)
4.end

Algorithm 1: Extraction Of Features

ExtractFeatures(frame f_k)
Input: Video frames
Output: Feature Set that contains the required features of the video
1.FaceDetection(f_k)
2.CaptureTime(f_k)
3.FeatureOccurrenceCount(f_k)

Algorithm 2: ExtractFeatures sub-routine

Embedding bits into the Video

The video from which the feature set is obtained is now subjected to LSB algorithm [4], for the purpose of embedding the secret bits into the video. With this, the information **I** is embedded into the video at the bit level.

Each video is made up a set of frames {f1, f2, f3, fn} denoted by F. Also, each pixel in the frame is a combination of RGB information. As the embedding is done at the pixel level, the RGB information of a pixel is modified with the secret bit and thus hiding it. For storing multiple bits, multiple pixels may be chosen whose RGB values may be modified..

Every pixel is a combination of RGB information. The color at a pixel is a result of that combination. Using LSB, the

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 30-35 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

data is embedded into this RGB information and thus, hiding the information.

This is best illustrated by the following example, where the attempt is made to embed a single bit into the Blue(B) part of the pixel. As only the Blue intensity information of the pixel is being modified, there will be a change only in the blue intensity. The following two figures show the raster values of a pixel before and after embedding of bits. The embedding shown is done in the Blue(B) part of the RGB information of the pixel.

(00110100 11010111 11000010)

Fig 4: Raster value of the pixel before bit embedding.

(00110100 11010111 11000011)

Fig5: Raster value of the pixel after bit embedding

There will be no apparently visible change in the frame as only a single bit of information is embedded in only one bit of the pixel. The algorithms that is used for this is explained below.

Input: Video ' V' that is composed of 'N' number of frames i.e., V= { f_1, f_2, f_3,…… f_N}
Output: Video 'V' that was embedded with the secret security bits
I_f'← Frame selection interval
S ← Set that contains security bits
1. foreach k ≤ N - I_f' **do**
2. k = k + I_f'
3. P← selected Pixel in f_k
4.P (R', G', B') **=LSB (** P (R, G, B), S')
5. end

Algorithm 3: Embedding Security Bits

Once the above steps are completed, the feature set is obtained and embedding of bits is completed. These can be used to carry out the process as illustrated below.

Mapping of Feature Sets

The feature set of the video whose legitimacy has to be tested is obtained by subjecting the video to Algorithm 1. This feature set obtained is mapped against the reference feature set already obtained, keeping in view, the time of occurrence constraint. If this matching rate exceeds the thresholdλ_{max}, then it could be possible that the video being analyzed is be a copied one. It is now, the second step is performed.

Checking for the presence ofembedded message

The video is now subjected to bit retrieval in order to see if it has any bits embedded at the pixel level. The bit sequence so obtained is compared against the reference message I. If the bit sequence obtained matches with the reference sequence I, then it can be concluded that the video is a legitimate one. If there is any mismatch between both the bit sequences, corresponding action like raising an alarm or preventing the video from being uploaded can be taken.

The flow of entire procedure is chalked out in the following flow diagram.

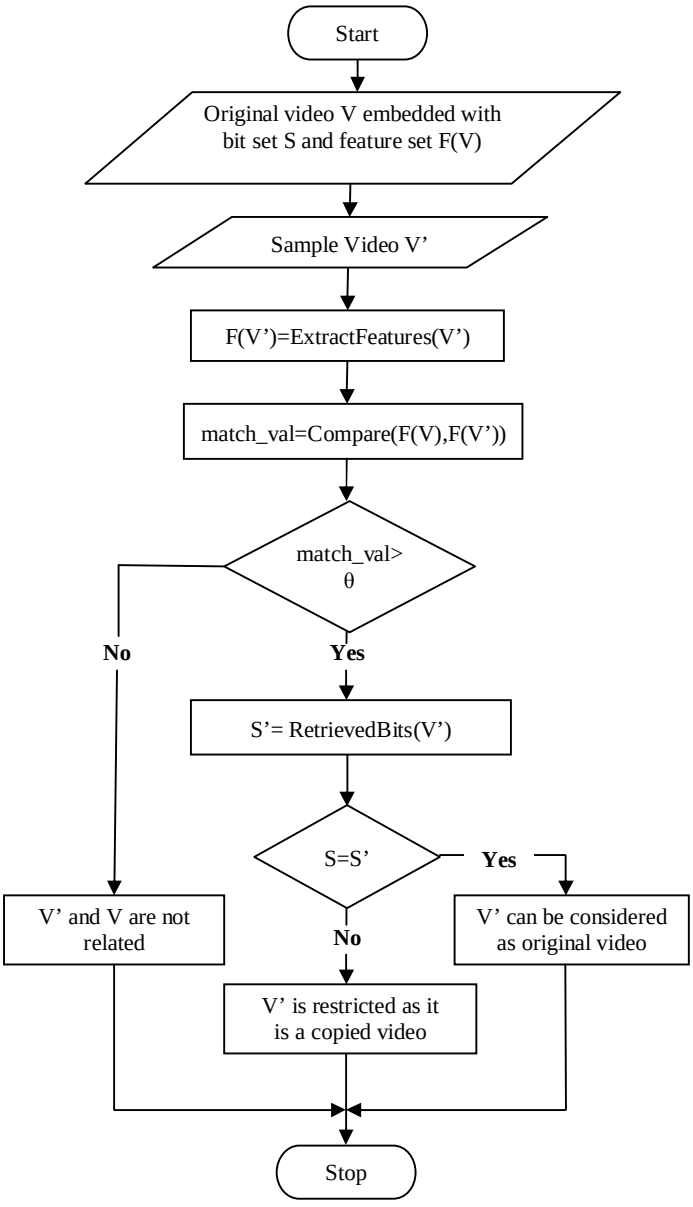

Fig6: Flow of entire procedure

The following flow diagram shows the entire flow of the approach that has been discussed.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 30-35 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

Input: Set of Security bits '**S**' and Feature sets **F(V)** and **F(V')**of both the videos V and V' respectively
Output: Determines whether V' is a copy of V or not
T← Threshold value

1. **foreach**feature F_i in F(V) and F(V') **do**
2. | Compare(F_i(V) , F_i(V'))
3. **end**
4. **if** match_percenatge≥ T
5. S'= BitsRetreival(V')
6. **if** S' != S
7. **Return** status that V' is a copied video
8. **else Return** status that V' is not a copied video
9. **else Return** status that V' is not a copied video

Algorithm 4: Feature Set mapping and retrieval of security bits

The embedding and bit retrieval into and from a frame can be known by the following figures.

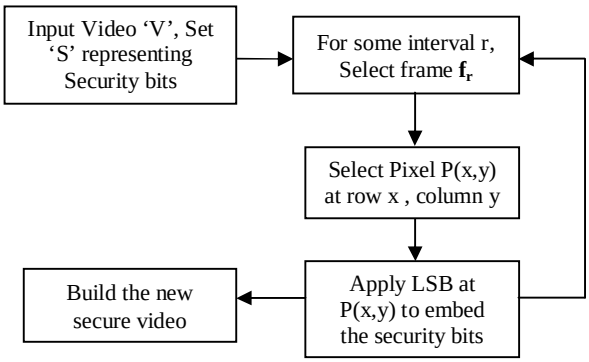

Fig 7: Embedding bits into a frame.

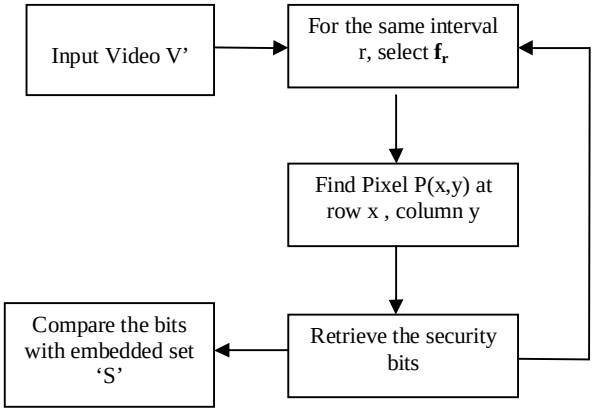

Fig 8: Retrieving bits from a frame.

RESULTS

The accompanying diagram shows the false acceptance and the false rejection rates for six of the example videos which we have considered. False acceptance speaks for the elements that may not be recognized as key facial characteristics yet still considered as a part of feature set and false rejectiondenotes vice-versa.

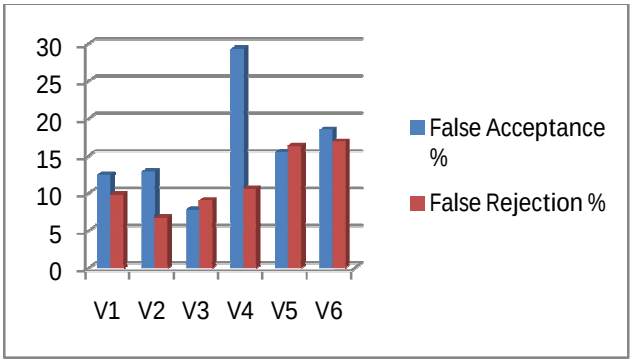

Fig 9: False Acceptance and False rejection rates.

Fig 10 shows the snap shot of the feature set.

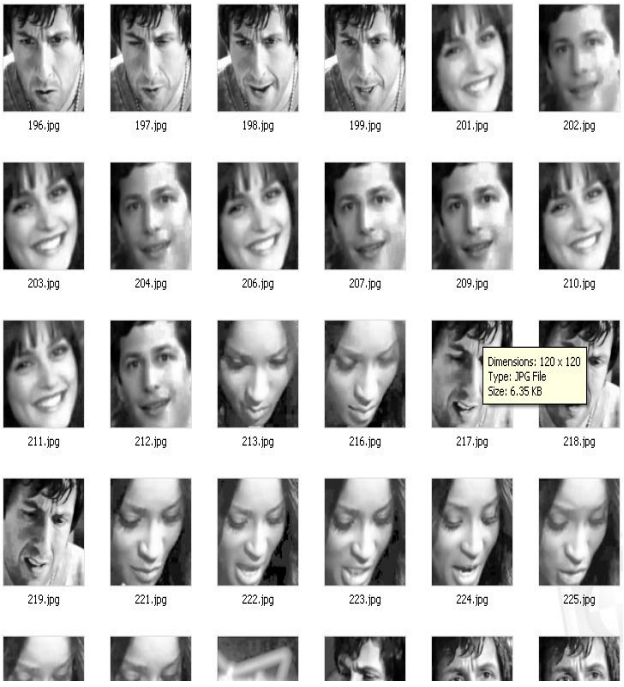

Fig 10: Snap shot of the feature set.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 30-35 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

00: 12:500000
00: 14:583333
00: 16:666667
00: 18:750000
00: 20:833333
00: 22:916667
00: 25:000000
00: 27:083333
00: 29:166667
00: 31:250000
00: 33:333333
00: 35:416667
00: 37:500000
00: 39:583333
00: 41:666667
00: 43:750000
00: 45:833333
00: 47:916667
00: 50.000000
00: 52.083333
00: 54.166667
00: 56.250000
00: 58.333333

Fig 11: Snapshot of time of occurrence of extracted features.

The comparison of copies of six videos are compared against the original ones and the percentage of the matches are obtained are tabulated in Table 1.

Table 1: Comparison of the features of the copied videos against the original ones.

Serial No.	Number Of Entries In The Feature Set Of Original Video	Number of Entries In The Feature Set Of Copied video	Match percentage(%) Obtained by comparing the Feature Sets
1	1701	1683	87.11
2	3247	3231	91.22
3	1213	1225	89.78
4	5032	4978	88.31
5	1221	1264	85.68
6	2167	2074	90.57

The visible difference between the frame containing the bits and the original frame is zero as we have embedded bits only into a single pixel in the frame.

Fig 12: Original Frame.

Fig 13: Frame containing a bit. (Represented with a green circle)

The results have shown that more the size of the bits we embed into the frames of the video more is the security.

Regardless of the fact that we apply bruteforce attack to break the secret message embedded into the video, the machines with the most advanced setup requires years to break through the method. Thus, as we increase the length of the secret message embedded into the video, this technique apparently turns to be invincible.

CONCLUSION

We proposed a technique which can be used as a standard at the server end and be used to prevent the unauthorized uploading and downloading of copyrighted videos. The basic assumption which is made here is that the original videos are built following the criteria specified. The basic drawback which is inherent in LSB is rectified here as we modify only a single bit of the pixel in the frame. Results have shown that, with increase in the length of the message that is embedded into the video, the probability of the system being cracked reduces many folds. Thus, this can effectively stand as a remedy to protect against copyright infringement.

REFERENCES

[1] Shailender Gupta, AnkurGoyal, Bharat Bhushan. “Information Hiding Using Least Significant Bit Steganography and Cryptography”. International Journal of Modern Education and Computer Science. Vol. 6, 27-34, June 2012.

[2] Gabriel MachariaKamau, Stephen Kimani, WaseruMwangi. “An enhanced Least Significant Bit Steganographic Method for Information Hiding”. Journal of Information Engineering and Applications. Vol. 12, No. 9, 1-12, 2012.

[3] VajihehSabeti, ShadrokhSumavi, ShahramShirani. “An adaptive LSB matching steganography based on octonary complexity measure”, Journal of Multimedia Tools and Applications, 2012.

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 30-35 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

[4] Vijay Kumar Sharma, Vishal Shrivastava. "A Steganography Algorithm for hiding image in image by improved LSB substitution by minimize detection". Journal of Theoretical an Applied Information Technology. Vol. 36, No, 1, 1-8, February 2012.

[5] Mazen Abu Zaher. "Modified Least Significant Bit (MLSB)". Computer and Information Science. Vol 4, Issue 1, 60-67, 2011.

[6] Souvik Bhattacharya and GautamSanyal. "Steganalysis of LSB Image Steganography using Multiple Regression and Auto Regression (AR) Model. International Journal of Computer Technology and Applications. Vol. 2, No. 4, 1069-1077, August 2011.

[7] Dr. EktaWalia, Payal Jain, Navdeep. "An Analysis of LSB & DCT based Steganography". Global Journal of Computer Science and Technology. Vol. 10, Issue 1, 4-8, April 2010.

[8] Chi-Kwong Chan, L M Cheng. "Hiding data in images by simple LSB substitution". Journal of Pattern Recognition Letters. Vol. 37, 469-474, 2004.

[9] Paul Viola and Michael J. Jones. "Robust Real Time Face Detection". International Journal of Computer Vision, Vol. 57, No. 2, 137-154, 2004.

[10] Ying Wang and Perre Moulin. "Steganalysis of Block-DCT Image Steganography". In Proc. IEEE Workshop on Statistical Signal Processing. 339-342, April 2010.

[11] Ismail Avcıbas, NasirMemon, BülentSankur, "Steganalysis Using Image Quality Metrics". IEEE Transactions on Image Processing, Vol. 12, No. 2, 221-229, February 2003

[12] Lienhart, R.; Maydt, J., "An extended set of Haar-Like feature for rapid object detection". In Proc. International Conference on Image Processing. Vol. 1, pp.I-900,I-903, 2002.

[13] J. Alex Stark. "Adaptive Image Contrast Enhancement Using Generalizations of Histogram Equalization". IEEE Transactions on Image Processing, Vol. 9, No. 5, 889-896, May 2000.

[14] Constantine P. Papageorgiou, Michael Oren, TomasoPoggio. "A General Framework for Object Detection". In Proc. Sixth International Conference on Computer Vision, 555-562, Jan 1998.

[15] Yoav Freund and Robert E. Schapire. "A decision-theoretic generalization of on-line learning and an application to boosting". in Proc. Second European Conference on Computational Learning Theory, 23-37, 1995.

[16] Ephraim Feig, ShmuelWinograd. "Fast Algorithms for the Discrete Cosine Transform" IEEE Transcations on Signal Processing. Vol. 40, No. 9, September 1992.

[17] http://www.go-gulf.com/blog/online-piracy/