ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient Data Encryption Technique in Video for Secret Sharing

Ms.D.S.Maind*
Student (M.tech), Computer Science & Engineering
Technocrats Institute of Technology,
Bhopal MP, India
dishamaind@gmail.com

Prof. Sini Shibu
Department of Computer Science & Engineering
Technocrats Institute of Technology
Bhopal, MP, INDIA
sinijoseph@hotmail.com

Abstract: The main objective of this paper is to develop a secret data sharing by using data hiding and extraction procedure for audio but by using uncompressed AVI videos. The videos are large so it can be transmitted from sender to receiver side over the network after processing the source video by using these Data Hiding and Extraction procedure securely. There are two different procedures, which are used here at the sender's end and receiver's end respectively. Secret communication is the main objective of this paper, so here we proposed some technique for sending data securely through Video.

Keywords: Data Encryption; Advance encryption standard; Security; data hiding; data hiding.

I. INTRODUCTION

A secret data can be share from sender to receiver side is not a new thing, there is several techniques available to share the data from sender to receiver side although here we discus another new technique using video, i.e., Encryption technique in video for secret sharing.

II. RELATED WORK

In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size. Enhanced Audio Steganography (EAS) is one proposed system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination. EAS uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message.

The basic idea behind this paper is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined[1]. Information hiding and secret communication is one of the most interesting and fascinating domains. This hiding method exploits some features of audio signals to be able to hide data from perception robustly. Every year researchers introduce their work and discuss how to make these techniques more and more robust against different types of attacks. In this article, we present an improved audio steganography approach that reduces distortion of the stego audio. Using the proposed algorithm, secret information is strongly protected from hackers and sent to its destination in a safe manner [2] .The main high resolution AVI file is nothing but a sequence of high resolution image called frames. Initially stream the video and collect all the frames in bitmap format
(Figure 1). And also collect the following information:

a. Starting frame: It indicates the frame from which the algorithm starts message embedding.
b. Starting macro block: It indicates the macro block within the chosen frame from which the algorithm starts message embedding.
c. Number of macro blocks: It indicates how many macro blocks within a frame are going to be used for data hiding. These macro blocks may be consecutive frame according to a predefined pattern. Apparently, the more the macro blocks we use, the higher the embedding capacity we get. Moreover, if the size of the message is fixed, this number will be fixed, too. Otherwise it can be dynamically changed.
d. Frame period: It indicates the number of the inter frames, which must pass, before the algorithm repeats the embedding. However, if the frame period is too small and the algorithm repeats the message very often, that might have an impact onto the coding efficiency of the encoder.

Apparently, if the video sequence is large enough, the frame period can be accordingly large. The encoder reads these parameters from a file. The same file is read by the software that extracts the message, so as both of the two codes to be synchronized. streaming the AVI video file into AVI frames I will like to use the conventional LSB replacement method. LSB replacement technique has been extended to multiple bit planes as well. Recently has claimed that LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. Still as my work is in high

© 2010, IJARCS All Rights Reserved

resolution video so I am getting a RGB combination of each pixel as in Figure2 hence if I consider one LSB I will have a choice of 3 bits for each pixel. That will overcome the clam And will give a higher security of the Data Hiding method [3].

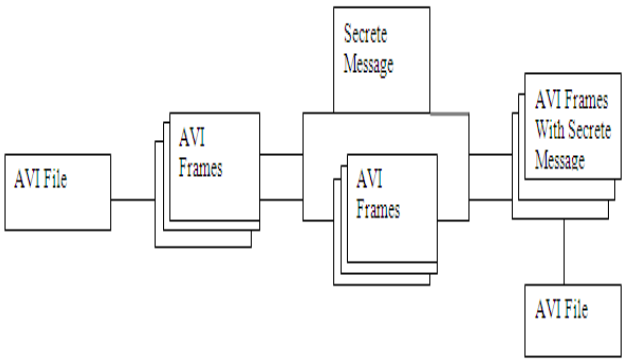


Figure 1. AVI video Streaming and Data Hiding Algorithm.

A steganographic algorithm in MPEG compressed video stream was proposed. In each GOP, the control information for to facilitate data extraction was embedded in I frame, in P frames and B frames, the actually transmitted data were repeatedly embedded in motion vectors of macro-blocks that have larger moving speed, for to resist video processing. Data extraction was also performed in compressed video stream without requiring original video. On a GOP by GOP basis, control information in I frame should be extracted firstly, then the embedded data in P and B frames can be extracted based on the control information. Experimental results show that the proposed algorithm has the characteristics of little degrading the visual effect, larger embedding capacity and resisting video processing such as frame adding or frame dropping [6] . In [7] a robust image steganography technique based on LSB insertion and RSA encryption technique has been used. Masud et.al has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. Other Examples of LSB schemes can be found in. Whereas EzStego developed by Machado embed information into an image in the GIF format. It sorts the palette to ensure the difference between two adjacent colors is visually indistinguishable. Tseng and Pan presented a data hiding scheme in 2-color images, it embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit. Proposes bit plane complexity segmentation (BPCS) method to embed information into the noisy areas of the image. These techniques are not limited to the LSB. Existing steganographic software, such as Steganos, S-tools and Hide4PGP , are based on LSB.

Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exists, where proposes the data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate file called key file. Whereas in selected LSB steganography algorithm is proposed. Other steganography techniques in uncompressed raw video, is illustrated [8], [9] and [10]. Steganography techniques for compressed video stream can be found in [11]. Another video steganography scheme based on motion vectors and linear block codes has been proposed in [12].

III. AUDIO DATA HIDING TECHNIQUES

Information hiding technique is a new kind of secret communication technology. The majority of today's information hiding systems uses multimedia objects like audio. Embedding secret messages in digital sound is usually a more difficult process. Varieties of techniques for embedding information in digital audio have been established. In this paper we will attend the general principles of hiding secret information using audio technology, and an overview of functions and techniques. As video file consists of several image sequences and audio, so considering the data hiding technique of audio will also apply for video data hiding [5].

A. Parity coding:

One of the prior works in audio data hiding technique is parity coding technique. Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

B. Phase Coding:

The phase coding method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is adjusted in order to preserve the relative phase between segments. Phase coding, when it can be used, is one of the most effective coding methods in terms of the signal-to perceived noise ratio. When the phase relation between each frequency component is dramatically changed, noticeable phase dispersion will occur. Phase coding is explained in the following procedure:

a. The original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded.
b. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases and Fourier transform magnitudes.
c. Phase differences between adjacent segments are calculated.
d. Phase shifts between consecutive segments are easily detected. In other words, the absolute phases of the segments can be changed but the relative phase differences between adjacent segments must be preserved. Therefore the secret message is only inserted in the phase vector of the first signal segment
e. A new phase matrix is created using the new phase of the first segment and the original phase differences.
f. Using the new phase matrix and original magnitude matrix, the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments back together.

To extract the secret message from the sound file, the receiver must know the segment length. The receiver can then use the DFT to get the phases and extract the information

© 2010, IJARCS All Rights Reserved

C. Spread Spectrum:

In a normal communication channel, it is often desirable to concentrate the information in as narrow a region of the frequency spectrum as possible in order to conserve available bandwidth and to reduce power. The basic spread spectrum technique, on the other hand, is designed to encode a stream of information by spreading the encoded data across as much of the frequency spectrum as possible. This allows the signal reception, even if there is interference on some frequencies. While there are many variations on spread spectrum communication, we concentrated on Direct Sequence Spread Spectrum encoding (DSSS).

D. D Echo Hiding:

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

IV. ALGORITHMS INVOLVED

With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important. Over the last few years several encryption algorithms have applied to secure video transmission. While a large number of multimedia encryption schemes have been proposed in the literature and some have been used in real products, cryptanalytic work has shown the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes. In this paper, a description and comparison between encryption methods and representative video algorithms were presented. With respect not only to their encryption speed but also their security level and stream size. A trade-off between quality of video streaming and choice of encryption algorithm were shown. Achieving an efficiency, flexibility and security is a challenge of researchers[4].

A. Symmetric key Algorithms:

In symmetric key encryption, the sender and receiver use the same key for encryption and decryption. As shown in fig 2.Symmetric key encryption is also called secret key, because both sender and receiver have to keep the key secret and properly protected. Basically, the security level of the symmetric keys encryption method is totally depend on how well the users keep the keys protected. If the key is known by an intruder, then all data encrypted with that key can be decrypted.

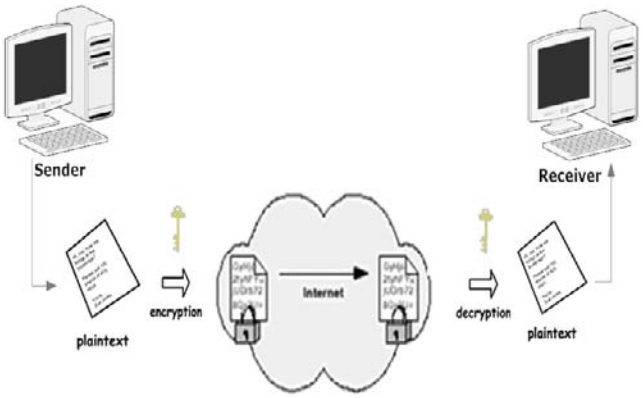


Figure 2. Symmetric key

This is what makes it more complicated how symmetric keys are practically shared and updated when necessary. Symmetric keys can provide confidentiality but they can not provide authentication, because there is no way to prove through cryptography who actually sent a massage if two people are using the same key. Due to that, with all the problem and defects that symmetric keys have they still used in many applications, because they are so fast and can be hard to break if using a large key size. Symmetric keys can handle a large amount of data that would take an unacceptable amount of time with asymmetric keys to encrypt and decrypt.

The most popular symmetric key algorithms are Data Encryption Standard (DES), Triple DES, and Advance Encryption.

a. The Data Encryption Standard (DES):

DES is one of the most important examples of a block cipher. The DES is widely used for encryption of PIN numbers, bank transactions, and the like. The DES is an example of a block cipher, which operates on blocks of 64 bits at a time, with an input key of 64 bits. Every 8th bit in the input key is a parity check bit which means that in fact the key size is effectively reduced to 56 bits.

b. Advance Encryption Standard (AES):

AES stands for Advanced Encryption Standard. AES is a symmetric key encryption technique which will replace the commonly used Data Encryption Standard (DES).AES provides strong encryption. AES is secure enough to protect classified information up to the TOP SECRET level, which is the highest security level. The AES algorithm uses one of three cipher key strengths: a 128-, 192-, or 256-bit encryption key (password). Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data, but also increase the complexity of the cipher algorithm. There a four basic step, called layers that are used to form the rounds:

a) The SubByte (**SB**) Transformation
b) The ShiftRow (**SR**) Transformation
c) The MixColumn (**MC**) Transformation
d) AddRoundKey (**ARK**) Transformation

© 2010, IJARCS All Rights Reserved

V. SYSTEM IMPLEMENTATION

A. Implementation:

This section we discuss how to split the uncompressed video into Images and audio. The system is carried out using Visual Studio 2008 software, using Dot net language. The Communication between the user and system are done through the user interface which is very easy for any user to handle. In the user interface it gives access to user to choose an input video. First the Video is taken as input.

B. Execution Detail:

a. GUI of system:

The following GUI system is used to split the video in Images and audio ,Figure 3 shows Login Form

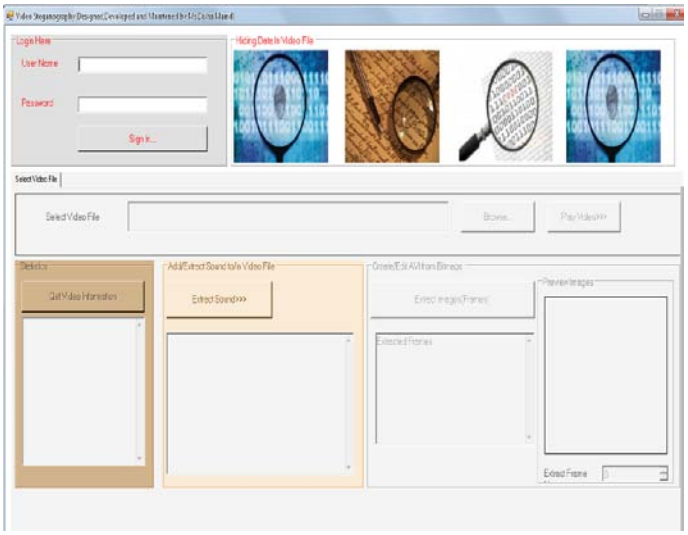


Figure 3. Login Form

b. Input Video:

Figure 4 shows Input uncompressed AVI video file .

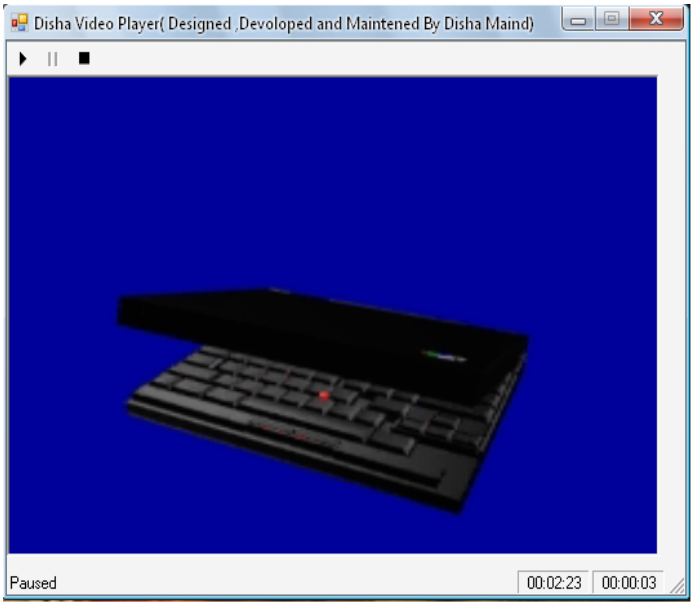


Figure 4. Input Video file

Step I:

Figure 5 shows the form which shows the selection of the input video.

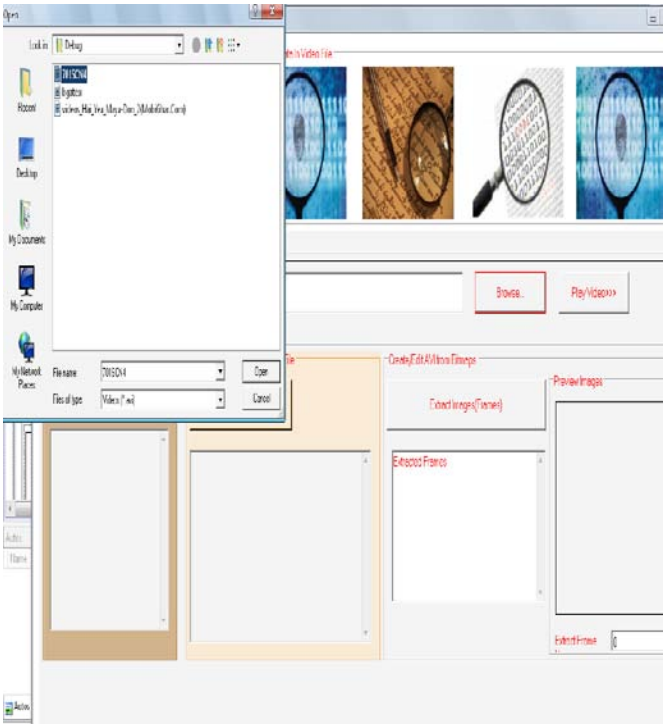


Figure 5. Input Video

Step II:

Once the video is selected, next step is to find the information about video for that I have created Get Information Button through this button display all the relevant information about the video likes width, height, number of frames, frame rate, sample per seconds, bits per samples, channels Figure 6 shows Get Video Information.

Figure 6. Get Video Information

Step III:

Figure 7 Extract sound from video file so to Extract Sound from the video I have created Extract Sound Button, which will creates Sound. Wav file format for audio

© 2010, IJARCS All Rights Reserved

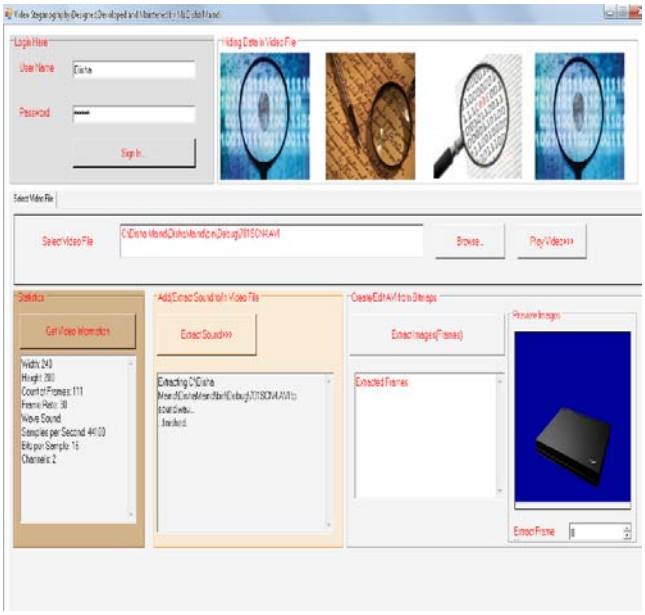


Figure 7. Extract sound from video file.

Step IV:

Once we extract sound from video, Figure 8 shows Extract images from video file. so that we can embed data into the video, as I have taken the 701SCN4.AVI video in these video total 111 images are present

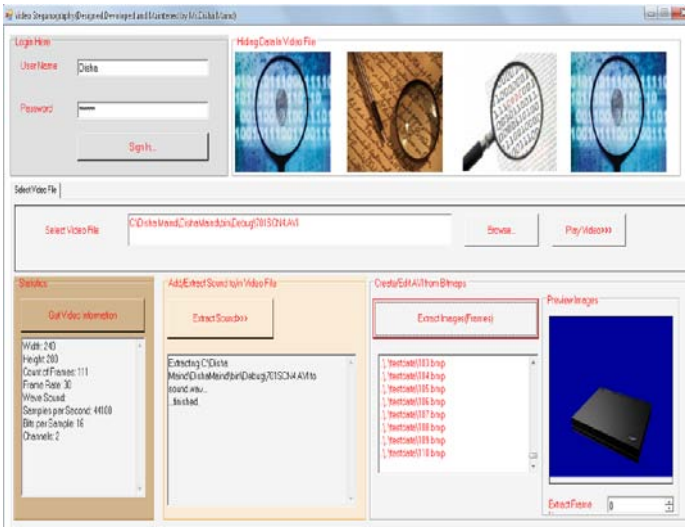


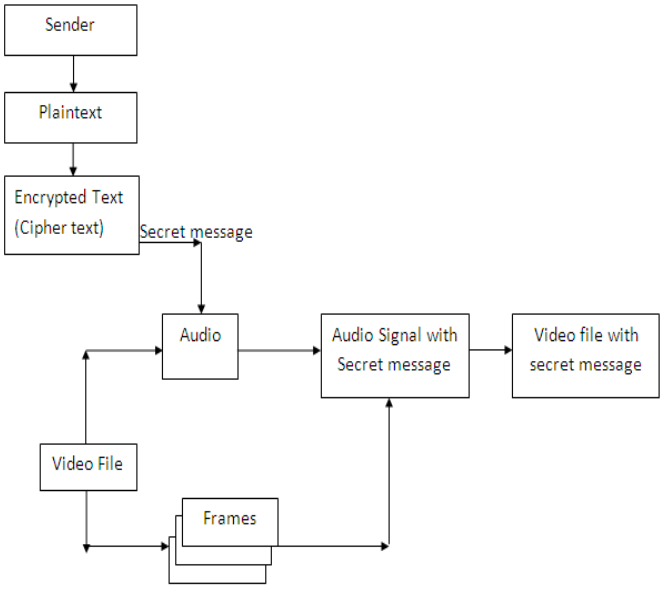
Figure 8. Extract images from video file.

VI. CONCLUSION

In this paper I have described how to split uncompressed video so that I can embedded encrypted data in to it, Efficient Data Encryption Technique in Video for Secret Sharing for encrypted data and able to embed data in video and then to decrypt the data and to rebuild the original video by removing the hidden Encrypted data.

VII. FUTURE WORK

In this paper I have discus how to split video into images and sound, next step is to embedded secret data into the audio file but this secret data will be a AES encrypted data so that the privacy of data will be maintained.



Sender Side Operation

VIII. REFERENCES

[1]. R Sridevi, Dr.A Damodaram, Dr. Svl.Narasimham," Efficient Method Of Audio Steganography ByModified Lsb Algorithm And Strong Encryption Key With Enhanced Security", Journal Of Theoretical And Applied Information Technology 2005 - 2009 JATIT.

[2]. Debnath Bhattacharyya, Tai-hoon Kim, Poulami Dutta," A method of data hiding in audio signal", Journal of the Chinese Institute of Engineers Volume 35, Issue 5, 2012

[3]. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas," Data Hiding in Video", International Journal of Database Theory and ApplicationVol. 2, No. 2, June 2009

[4]. M. Abomhara, Omar Zakaria, Othman O. Khalifa," An Overview of Video Encryption Techniques" , International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201

[5]. Poulami Dutta," Data Hiding in Audio Signal: A Review", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009

[6]. Changyong Xu, Xijian Ping, Tao Zhang," Steganography in Compressed Video Stream" ,Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) 2006 IEEE

[7]. Fillatre. L, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, IEEE Transactions on Signal Processing, Volume 60, Issue:2, pp. 556-569, Feb, 2012

[8]. A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas, Data Hiding in Video in International Journal of Database Theory and Application Vol. 2, No. 2, pp. 9-16, June 2009.

[9]. J. J. Chae, B. S. Manjunath, Data Hiding in Video, Proceedings of the 6th IEEE International Conference on Image Processing, pp.311-315, 1999.

[10]. Melih Pazarci, Vadi Dipcin, Data Embedding in Scrambled Digital Video, in Proceedings of the 8th IEEE International Symposium on Computers and Communication, pp. 498-503, 2003.

[11]. A. Giannoula, D. Hatzinakos, "Compressive Data Hiding for Video Signals", in Proceedings of International Conference on Image Processing, pp. I529- I532, 2003.

© 2010, IJARCS All Rights Reserved