Digital Video Steganography Technology For Security Application

E. Anna Devi
Research Scholar, Department of ECE, Sathyabama Institute of Science and Technology, Chennai-600119.

R. M. Joany
Research Scholar, Department of ECE, Sathyabama Institute of Science and Technology, Chennai-600119. mariajoany@gmail.com

S. Yogalakshmi
Research Scholar, Department of ECE, Sathyabama Institute of Science and Technology, Chennai-600119.

L. Magthelin Therase
Research Scholar, Department of ECE, Sathyabama Institute of Science and Technology, Chennai-600119.

Abstract - The paper proposes a technique on the digital video steganography. Various techniques are employed in order to achieve a higher secure data transmission these includes the cryptography, watermarking and steganography the steganography finds its application in the audio-video synchronization, copyright control and T.V. broadcasting specially in military areas the paper analyses the various improvements made in the security of the data transmission as well as the various methodologies adapted in achieving the same. the major difference between the steganography and the cryptography is the latter has the cipher text which is coded and then transmitted while the former is embedded within a image or in a video frame so as to achieve the intended use.

Keywords - Encryption, Cryptography, LSB, steganography adaptive lsb, watermarking, AES.

1. INTRODUCTION

With the improvement and with the advancement in technology and events security plays a major role. Where the privacy concern of an individual has increased. Thus it becomes mandatory for an individual to protect his privacy security and this paper proposes a methodology where the images are hidden or embedded with in images or with in the video frame which finds a large application in security fields and military applications as well as the proposed technique makes use of RC7. Encryption which is far more better the conventional method also the image embedded this paper gives an insight about the various advantages as well as the disadvantages that are applicable in the industry, using the MATLAB the application is processed.

Steganography is classified in to two types as 1. Linguistic steganography 2. Technical steganography also watermarking is one such technique which is used in the data transmission which achieves a higher secrecy the watermarking can be classified into 2 types they are 1. Robust 2. fragile the block diagram of the steganography both in the embedding as well as the extraction side is as shown below in the fig.
2. **Theoretical Framework**

2.1 **DOUBLE CODING MECHANISM FOR ROBUST AUDIO DATA HIDING IN VIDEOS**

The author of this paper describes about the double coding mechanism by which two codes are used such that it becomes complex to track down the original information content this is performed by pseudo codes and morse codes the performance of the system is measured in terms of mean square error(MSE) And peak signal noise ratio(PSNR) initially the transformation between the domains are made (i.e) from transform domain to spatial domain. The spatial domain as a disadvantage of more payload the mathematical tools used in transformation of the domain fourier transform discrete cosine transform and the discrete wavelet transform .the conclusion of this paper better methods can be adopted and the loopholes as well the paper as a better MSE and PSNR further more write after the embedding of data the resultant image is compressed and even on compressing of the resultant image the method prof to be effective
2.2 AN IMPROVED IMAGE STEGANOGRAPHY TECHNIQUE BASED ON MSB USING BIT DIFFERENCING

On conventional steganography the data is embedded with in the video or image frame the LSB as know vitel information so that data to be hidden is concealed within the LSB and then it is transmitted this paper overcomes the conventional steganography by using the MSB . the different formats of data that can be processed are image takes and audio the theratical frame work used in this MSB technique the bite 5 shows the secret bit based on the difference in bit 5 and 6 of thr cover image three important parameters in the steganography is discussed in this paper which are 1.payload capacity 2.robustness 3.security where the payload capacity plays an important role in spatial domain the difference between in cryptography steganography is also discussed where as in a cryptography cipher text is used but in a steganography the data is emdedded and hidden to the rest of them other than the intentent recipient the conclusion of this paper is that MSB based data hiding technique is more efficient and provides a better PSNR ratio over the conventional way

2.3 MULTICLASS DETECT OF CURRENT STEGANOGRAPHIC METHODS FOR JPEG FORMAT BASED RE-STEVENOGRAPHY

The goals of JPEG Image steganography detection are not only distinguished cover images (the normal images) and stego images, but also determine the steganography algorithms of the stego images, and extract the embedded information, of which the preconditi on is to determine the image steganography algorithm. The changes of storage size from re-steganography to image is much smaller than that from steganography to image. Specifically, the storage size of JPEG image, with the first JPhide steganography, is reduced about 50% than before; but with the second JPhide steganography to the image, the change of the storage size was relatively small, almost no change. an effective steganalysis multi-class classification algorithm in this paper, which outperforms the state-of-the-arts in detecting the modern steganographic methods plan to further improve the detection reliability of the proposed steganalysis algorithm.

Firstly, expanding the application range of the algorithm, we want the proposed algorithm outperform in other steganographic methods: MB1, MB2, SSIS and H4PGP. Secondly, we want the algorithm to further simplify and run with more high efficiency.

2.4 THE VIDEO HIDING TECHNIQUE BASED ON DWT AND GENETIC ALGORITHM WITH BOOLEAN FUNCTIONS

The author of the paper makes use of the discrete wavelet transform(DWT) wavelet is the short lived pulse unlike a sinusoidal signal. The wavelets can be classified in to many types based on that amplitude and the shape of the waveform sum of them are by orthogonal 2.2,daubauchies so this paper deals with the DWT as a tool in data hiding technique .DWT is useful in digital globe the activity of wavelet transform is analysed to the attacks the data hiding technique they are by preventing from the hackers or attackers.from this paper the embedding image Is randomized and is moved towards the higher LSB layers the conclusion of this paper is that gives us DWT and the generic algorithm for hiding data effectively and efficiency.

2.5 A NEW WATERMARKING APPROACH FOR REPLAY ATTACK DETECTION IN LQG SYSTEMS

They are major three techniques in data hiding one such technique is watermarking the author of this paper deals with the watermarking is a process of hiding data embedding in a noise tolerant signal such as an audio video or image data the digital information is hidden in a carrier signal both the steganography and digital watermarking employee’s steganography techniques to embedded data in a noise signal. The watermarking technique is combined along with the steganography and it enhance the PSNR and provides better solution for the noise attack further. this paper gives an idea about the classification of steganography which is of two types linguistic and technical for the more watermarking is divided into two types robust and fragile various parameter like PSNR and MSE and embedding capacity for evaluated and the results are discussed in the paper
2.6 CONTENT-ADAPTIVE PENTARY STEGANOGRAPHY USING THE MULTIVARIATE GENERALIZED GAUSSIAN COVER MODEL

The vast majority of steganographic schemes for digital images stored in the raster format limit the amplitude of embedding changes to the smallest possible value. In this paper, the author investigates the possibility to further improve the empirical security by allowing the embedding changes in highly textured areas to have a larger amplitude and thus embedding there a larger payload. The approach is entirely model driven in the sense that the probabilities with which the cover pixels should be changed by a certain amount are derived from the cover model to minimize the power of an optimal statistical test. The embedding consists of two steps. First, the sender estimates the cover model parameters, the pixel variances, when modeling the pixels as a sequence of independent but not identically distributed generalized Gaussian random variables. Then, the embedding change in the probabilities for change in each pixel by 1 or 2, can be transformed to costs for practical embedding using syndrome-trellis codes, and they are computed by solving a pair of non-linear algebraic equations.

3. CONCLUSION AND FUTURE WORK

Hence this paper analyses the various complexities and the problems that are associated with the Digital Video Steganography technology for security applications along with the remedies that are solved in the consecutive papers the future work of this can be extended to design an hardware that is capable of making video steganography which is intended for the use by a general consumer.

REFERENCE

[1] Shaikh Shakeela, P. Arulmozhivarman, Rohit Chudiwal, Samadrita Pal Double Coding Mechanism for Robust Audio Data Hiding in Videos Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on 20-21 May 2016.
[2] AmmadUl Islam, Faiza Khalid, Mohsin Shah, An improved image steganography technique based on MSB using bit differencing Innovative Computing Technology (INTECH), 2016 Sixth International Conference on 24-26 Aug. 2016.
[3] G. Sowmya; K. Meghana; B. Subbarayudu; R. Ch. A. Naidu; G. Keerthi Wangqiang Niu The video hiding technique based on DWT and genetic algorithm with boolean functions 2016 2nd International Conference on Next Generation Computing Technologies (NGCT) Year: 2016 Pages: 843 – 849.
[4] Steganography over video file by hiding video in another video file, random byte hiding and LSB technique Rachna Patel; Mukesh Patel 2014 IEEE International Conference on Computational Intelligence and Computing Research Year: 2014 Pages: 1 – 5.
[5] Datta, Biswajita, Souptik Tat, and Samir Kumar Bandyopadhyay, "Robust high capacity audio steganography using modulo operator." International Conference on Computer, Communication, Control and Information Technology (C3IT), IEEE, (2015, December 21-24), Himachal Pradesh, India.
[6] Guohua Wu, Xiaodong Zhou, 2008. “A Fast Audio Digital WatermarkMethodBasedonCounter-propagation Neural Networks”, International Conference on Computer Science and Software Engineering, pp. 583-586 Hartung, F. and Girod, B. 1998.
[7] Watermarking of uncompressed and compressed video, Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 66 (3): 283-301. Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and TeMing Tu.;
[8] A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia, VOL. 3, NO. 2, JUNE 2008 Lee, Y. K. and Chen, L. H. 2000.
[9] High capacity image steganographic model. IEE Proceedings on Vision, Image and Signal Processing, Vol. 147, No.3, pp. 288-294. Maher El’Arbi et al. 2006. “Video Watermarking Based On Neural Networks”, ICME, pp. 1577-1580.
[10] S.Karthikeyan, S.Jayashri, “Energy Utilization Strategies using Novel Approach in Wireless Sensor Networks”, International Conference on Software Engineering and Mobile Application Modelling and Development, Dec 2012, pp: 1-5.
[11] S.Karthikeyan, S.Jayashri, “Energy Efficient System for Heterogeneous Wireless sensor Networks”, European Journal of Scientific Research, Volume 72, No 4 March 2012, PP:599-607. ISSN: 1450-216X.
[12] S. Karthikeyan, S. Shannugapriya and S. Jayashri, “Sub-header Transmission of Heterogeneous Data by Cloned Agent to Android Mobile”, Research Journal of Applied Sciences, Engineering and Technology, 8(1): pp. 24-34, 2014

[13] S. Pavithra, S. Karthikeyan, V. J. K. Kishor Sonti, S. Jayashri, “Competent Realization of Co-operative spectrum sensing in cognitive radio systems”, International journal of Engineering systems modeling and simulation, Inder science publishers, Vol. 7, No. 2, pp 103-110 2015.