OPTIMIZE TECHNIQUE FOR INCREASING DATA HIDING CAPACITY AND SECURITY USING BIT FLAP AND HIGHER LSB MECHANISM

Miss. Komal D Lahane
Master of Engineering
Computer Engineering Department.
Shri Sant Gajanan Maharaj College of Engineering,Shegaon
Sant Gadge Baba Amravati University,India

Prof. N. M. Kandoi
Head, CSE.
Shri Sant Gajanan Maharaj College of Engineering,Shegaon
Sant Gadge Baba Amravati University,India

ABSTRACT

An uncompressed video secure stegnography formula is projected within the formula, embedding and detection operations square measure each dead entirely within the uncompressed domain, with no would like forth compression method. The new criteria using applied math physical property of contiguous frames is employed to regulate the embedding strategy and capability, that will increase the protection of projected formula. Therefore, the collusion resistant properties square measure obtained. Video steganalysis with closed-loop system feedback manner is style as a checker to seek out obvious bugs. Experimental results showed this theme is applied on uncompressed video stegnography with high security properties.

Keywords:- Stegnography, steganalysis, stego-image.

I. INTRODUCTION

Stegnography is that the transmission of a secret message hidden at intervals a normal carrier while not revealing its existence. The instrumentation(cover file) could also be a digital still image, audio file, or video file.

Once the key message has been embedded, it should be transferred across insecure lines or announce publically places. Usually, the information rate of cowlt knowledge transmission exploitation steganography is low so as to stay the quit data impalpable at intervals the cover medium. This rate is somewhat proportional to the amount of the quilt medium. For this reason, digital video may be a convenient alternative for stegnography. Nowadays, given the high degree of collaboration and cooperation in trendy data system like rising multimedia system sensing element networks, covert communications becomes a larger threat to rhetorical analysis than ever. It's imperative to analyze ways to notice and discourage covert communications like stegnography in multimedia system networks that acquire extremely related to knowledge. This paper can concentrate on the actual downside of the compressed video stegnography.

Generally speaking, digital video seems in two main distinct coding formats: the uncompressed and also the compressed. The most well-liked compressed format far and away is motion salaried compressed video,

specifically the wide accepted common place MPEGx. It achieves compression through the elimination of temporal, abstraction and applied mathematics redundancies with this compression operation. The video bit-stream consists of variable length codes(VLC) that represent numerous video segments. For video stream sometimes being offered in compressed type, stegnography algorithms that aren't applicable in compressed bit-stream would need complete or a minimum of partial decompression[1-4] this is often associate degree uncalled for burden best avoided. He If the need of strict compressed domain stegnography is to be met, the stegnography has to be embedded within the compressed domain. Nowadays, there area unit great amount of video watermarking algorithms been projected and a few of them area unit applied for compressed video[5-9]. To be helpful, a stegnographic technique mustn't be simply detectable. If the existence of secret message are often detected with a likelihood over random estimation, the corresponding steganography technique is taken into account to be invalid. Almost like cryptography, stegnography might suffer from the attack methodology(steganalysis). A lot of the analysis add the sphere of steganalysis has been dispensed on pictures. One approach is predicated entirely on the primary order statistics and is applicable solely to unchanged embedding. Another major stream is predicated on the conception of blind steganalysis, that is created by blind classifiers. The classifiers ought to be trained to be told the variations between cowl and stego-image options initially.

The strength of information activity gets amplified if it combines with the cryptography. In knowledge activity, the terminologies used are cover-image, hidden image, secret message, and secret key and embedding algorithmic program. Cover-image is that the carrier of the message likes audio file, video or image. Cover-image carrying the embedded secret knowledge is that the hidden image. Secret message is that the data that's to be hidden during a cowl image. The key secret is a costumed plants the message reckoning on the activity algorithmic program [2]. The embedding algorithmic program is that the manner, that is employed to plant the key data within the cover image.

The securities of the transformation of hidden knowledge are often obtained by 2 ways: Cryptography and Knowledge activity. Mixes of the 2 technique are often accustomed increase the information security. Cryptography may be a technique during which the message is modified in such the way in order that no knowledge are often disclosed if it's received by associate wrong doer. Whereas in knowledge activity, the key message is embedded into a picture usually known as cowl image, and so sent to the receiver who extracts the key message from the quilt message. Once the key message is embedded into cowl image then it is known as a hidden image [6]. The visibility of this image shouldn't be distinguishable from the quilt image, in order that for wrongdoer it nearly becomes not possible to find any embedded message

Here we have a tendency to work the info concealment technique that is reversible in nature. Therefore it's termed as Reversible information hiding technique. In severable

reversible information hiding technique first of all a content owner encrypts the first uncompressed image then an information hider compress the image to create house to accommodate some further information. Reversible information concealment could be a technique to engraft further message into some distortion-unacceptable cowl media, such as military or medical pictures, with a reversible manner in order that the original cowl content is utterly renovated once extraction of the hidden message. As a good and common means for privacy protection, cryptography contains encryption and decryption. It converts the standard signal into incomprehensible information, in order that the final signal processing generally takes place before cryptography or once decryption.

II. LITERATURE SURVEY

For finding out the ideas of video stegnography and watermarking technique we've surveyed several latest papers. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and MaricelO.Balitanas[2], the most necessities of any information activity system area unit security, capability and strength. It's terribly troublesome to archive of these factors along as a result of these area unit reciprocally proportional to every different. Authors have focuses on increasing security and capability issue of knowledge activity. The information activity technique uses high resolution digital video as a canopy signal. It provides the power to cover a major quality of information of knowledge creating it totally different from typical data activity mechanisms. They need used the big payloads like video in video and movie in video as a canopy image.

Ahmed Ch. Shakir[1], the confidential communications over public networks are often done exploitation digital media like text, images, audio and video on the network. Merely activity the contents of a message exploitation cryptography wasn't adequate activity of message ought to offer an extra layer of security.To supply the additional security the author steered the new procedures in stegnography for activity ciphered data within a digital color picture image. He has used quadratic technique looking on the locations over by the binary image, beside of public key cryptography.He had over that the conjunction between cryptography and stegnography manufacture immune data.

Andreas Westfeld and Gritta Wolf [3], during this work author have delineate a steganographic system that embeds secret messages into a video stream. Ordinarily the compression ways area unit utilized in video conferences for securing acceptable quality. However sometimes, compression ways area unit lossy as a result of reconstructed image might not be identical with the initial. There area unit some downside of compression and information embedding technique. Signal noise and irrelevancy area unit common samples of information embedding. However compression ways try and take away signal noise and irrelevancy. If signal is compressed additional, then there area unit fewer potentialities of knowledge embedding. The author have solved this downside, they need investigated a typical signal path for information embedding. During this formula security is established by indeterminism inside the signal path.

Sherly A P and Amrita PP[16], during this

paper author have projected a brand new compressed video steganographic theme. During this theme the information is hided in compressed domain. The novel embedding technique Triway pel worth Differncing(TPVD) is employed to extend the capability of the hidden secret data associated for to providing an impalpable stego-image for human vision. This formula are often applied on compressed videos while not degradation in visual quality.

Saurabh Singh and Gaurav Agrawal[11], have given a unique approach of activity image in an exceedingly video. During this approach, one LSB of every pel is replaced by the one little bit of secret message. Thus it's terribly troublesome to search out that image is hidden within the video of thirty frames per second. The analysis is extremely troublesome as a result of every row of image pixels is hidden in multiple frames of the video. The interloper needs full video to unhide image. Authors have delineate the LSB formula during this paper. The projected formula is extremely helpful in causation sensitive data firmly.

III. ANALYSIS OF PROBLEM

Now a days, a current challenge consists to insert data in encrypted photos as a result of the entropy of encrypted image is largest, the embedding step like noise is not potential by victimization common place data concealing algorithms. New arrange is to use reversible data concealing algorithms on encrypted photos by want to induce eliminate the embedded data before the image cryptography. There's one another drawback if either concealing key or cryptography key's leaked then welcome person can extract or rewrite the image through cryptography key. Another draw back found is that, the key use for encrypting the image and data concealing is same. That the user United Nations agency is alert to the key usefor cryptography can access the embedded data and original data. We tend to are able to retrieve the primary image from encrypted image once extraction or removing the data hidden at intervals the image. The content owner and data hider share constant cryptography key for cryptography of image and data concealing. Upto this there's no provision of choosing the key and extra encoded code time consumption. There are varied data concealing programs on the market variety are superb in every respect sadly, many of them lack usable interfaces or contain many bugs, or inconvenience of a program for different operative systems.

IV. CONCLUSION

The general aim of this to extend the information concealing capability and conjointly the safety by victimization higher LSB technique. Video steganography may be a technique to cover any quite files into a carring video file. The utilization of the video based mostly stegnography are often additional eligible than alternative multimedia system files, owing to its size and memory needs the smallest amount important bit (LSB) insertion is a vital approach for embedding info in an exceedingly carrier file. Least important bit (LSB) insertion technique operates on LSB little bit of the media file to cover the data bit. By victimization this capability of embedding bits into the duv timage are often increased.

Thi system is to produce a decent, economical technique for concealing the information from hackers and sent to the destination in an

exceedingly safe manner. So it are often all over that Higher LSB and bit undulation in planned technique are often used which is able to bring numerous blessings which might be used for variety of functions aside from coated communication. The presents a theme that may transmit giant quantities of secret info and supply secure communication between two communication parties.

REFERENCES

[1] Amr A. Hanafy, Gouda I. Salama, Yahya Z. Mohasseb, "A Secure Covert Communication Model Based on Video Steganography", Military Communications Conference, IEEE, Pages No. 1 – 6, 16-19 Nov., 2008

[2] Arup Kumar Bhaumik, Minkyu Choi, RosslinJ.Robles, and MaricelO.Balitanas," Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009

[3] Andreas Westfeld and Gritta Wolf," Steganography in a Video Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998

[4] Cheng Cheok Yan, "Introduction on Text Compression Using Lempel, Zip, Welch (LZW) method"

[5] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", i-manager's Journal on Software Engineering, Vol. 4 l No. 3 l January - March 2010 65,pp.65-71

[6] D.P.Gaikwad and Dr. S.J.Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA-PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai.

[7] Richard E. Woods & Rafael C. Gonzalez "Digital Image Processing"Book

[8] F 5 algorithm implementation: 2009, Fridrich, J.R.Du, M. Long: Steganalysis in Color Images, Binghamton, 2007

[9] Neil F. Johnson and SushilJajodia,"Exploring Steganography: Seeing the Unseen", George Mason University.

[10] S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ," International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397

[11] Saurabh Singh and Gaurav Agarwal,"Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003

[12] Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-1-4244- 7432-5

[13] Y. J. Dai., L. H. Zhang and Y. X. Yang.: A New Method of MPEG Video Steganographying Technology .International Conference on Communication Technology Proceedings (ICCT), 2003

[14] D.-C. Wu and W.-H. Tsai: A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003

[15] F Hartung., B. Girod.: Steganoing of

uncompressed and compressed video, Signal Processing,Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66 (3): 283-301

[16] Sherly A P and Amritha P P,"A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.230767