iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Video steganography -Information Security Perspective

Boopathy. R[1], Dr.Dhaya.R [2] ,Dr.Ramakrishnan.M [3],Dr.Victor.S.P [4]
[1] & [2] *Department of Computer Science & Engineering, Velammal Engineering College, Chennai, Tamilnadu, India*
[3] *Head of Computer Science, Madurai Kamarajr University*
[4] *Research Director, Xavier College, Pallayamkottai*

Abstract—Security in digital multimedia content is inevitable in the era of Internet .Unauthorized person should not be able alter or receive the message .To address this issue many security mechanisms have evolved like encryption, watermarking, and steganography. The most trusted and reliable method of secured communication is Steganography. It is the science of covert communication which usually carries data in image, audio or video and conceals the existence of the data in that way it differs from cryptography. However this technique could be misused for ill intentions also. This paper gives a survey of current steganography techniques and proposed new method of data hiding using Saliency map technique .Robustness, Im-perceptibility and capacity are the features considered in designing a steganography system. Bank transactions , Military communications , Government ,Business secrets , medical image transactions , individual or group communications are some of the major areas in which steganography is being used. Steganalysis is the science of breaking the steganography which is not concentrated in this paper, but this paper concludes with recommendation of robust steganography system that withstand against steganalysis and statiscal attacks. The metrics for evaluating the performance of Steganography is also emphasized in the concluding remarks.

Keywords: Digital Steganography, Spatial domain, frequency domain, Spread Spectrum, Network Steganography, Saliency map.

I. INTRODUCTION

Secured Communication drew the attention of society in 1993 where users of computer systems were alerted to dangers when a set of programs called *sniffers* were placed on many computers run by network service providers and recorded login names and passwords. In 1998 using a program called worm nearly 5000 computers were stalled for 4 hours. On September 11, 2001 militants seized control of four flights…. There were flown buildings and a fourth crashed,In the aftermath , the security and reliability of many aspects of society drew renewed scrutiny .Many hackers maliciously or frivolously corrupting or destroying information have taken millions of dollars to amass .In mid 1980s mainframe and mid-level computers dominated the market , security problems and solutions were focused in terms of securing files or process on single system. With the rise of networking and the internet , the arena has changed. Workstations and Servers now dominate the market .Computer security problems and solutions now focus on the network environment. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. For example military and civilian institutions including bank transactions in the government often restrict access to information to those who need that information .Trade secrets , Personally Identifiable Information such as credit or and debit card numbers , Protected health Information and medical image transactions could be protected using Steganography. Confidentiality is the concealment of information or resources . Cryptography is one mechanism which preserves confidentiality .Cryptography which scrambles data to make in incomprehensible. A cryptographic key controls access to scrambled data , but then the cryptographic key itself becomes another datum to be protected.

Resource hiding is another aspect of confidentiality ,Concealing the message using technique called Steganography is the new research area in the field of information security & data hiding .Breach of security should not occur in the protected systems. Threat is potential violation of security . Attackers executes actions that causes violation .Threats normally divided into four categories called disclosure, deception, disruption and usurpation. snooping , modification or alteration , Masquerading or spoofing , repudiation of origin, denial of receipt , delay are the major threats.

Even though Steganography is authentic way of sending secret messages , the same technique could be used by militants of illegal transfer of data, to avoid this research on Steganalysis has evolved . The Process of Steganalysis is to find out the suspected stego media and then try to recover the hidden message. Firewalls, Content Monitoring Systems , intrusion detection and pre-

vention systems , and data leake prevention system unable to detect /protect /restrict the file that contains embedded child pornography, in such a cases Steganalysis easily find out the existence of hidden image in any file .

Watermarking also plays major role in securing digital media files .Copyright protection is the major issue while transformation of digital media files in the internet. Watermarking is of two types viz visibile and invisible (imperceptible) watermarking .The outcome of watermarking is tamper proofing in which hacker cannot remove or replace the original message which ensures the ownership of file .The goal is to protect the copyrights of owner by means of one to many communications . Robustness and tamper proofing are the Properties of any watermarking algorithm. In [1] authors presents a new scaling based image watermarking scheme which exploits the properties of human visual systems . The information is hidden in high-entropy blocks and for decoding the watermark new maximum-likelihood decoder is used for each block. Here low pass wavelet coefficients are utilized for data embedding along with this new decoder plays a major role in ensuring the robustness. Now a day's many illegal copies of cinema are found on the internet before official release or day after the release .Spread Spectrum based watermarking technique is used to protect digital cinema[2].It judges the position of seat in a theatre and detects when and where cinema was captured .Time and location information was estimated by position estimation model(PEM).

II. LITERATURE SURVEY

A. Introduction

Many authors have already contributed on Steganography .This Literature survey gives the idea of new researchers and related works accomplished by others .This section demonstrates our understanding of the relevance and our ability to do problem definition .

B. General Survey

Abbas Cheddad et al (2010) conducted a Survey and analysis of current digital steganography methods and authors suggested a common guidelines and suggested a objected oriented embedding mechanism. The major techniques like adaptive steganography, DCT,DWT are less prone to attacks but having less capacity when compares to spatial domains. Some authors suggests robustness is essential for watermarking not for steganography while others suggests that robustness is essential for steganography. Survey reveals that familiar image should not be selected as carrier image. Alternative method to achieve high capacity is usage of video as carrier file. The most useful application of steganography is applying intelligent restricted Content Based Image Retrieval (CBIR).

Nan-I Wu et al(2011) considered and implemented a method of data hiding using pixel value differentiating which leads to large payload capacity. They introduced base decomposition scheme which offers a base fare for each degree to construct a two base notational system. Authors claimed that their method outperforms others by having higher PSNR and surveyed against RS steganalysis attack, Minimum distortions maintains the features of cover image , different metrics like Minkowki summation, Watson metric , metric based on Structural SIMilarity (SSIM) were used to test the performance .

C. JPEG Steganography

In [2] for JPEG2000 baseline system high capacity Steganography scheme is proposed. This Scheme uses bit-plane encoding procedure to hide high volume of data after embedding. Bit stream truncation and redundancy measurement were the two contributions in that paper. The wavelet coefficients greater than a given threshold were chosen as candidate embedding points.

Linjie Guo et al (2014) suggested a method for JPEG steganography using Uniform Embedding Distortion Method (UED) .Discrete Cosine Transformation (DCT) is used for quantization , syndrome trellis coding is incorporated to reduce the distortions so that less statistical detect ability and high embedding efficiency is also achieved. Uniform embedding is the concept related to spread spectrum methodology by means of spreading embedding modifications to DCT coefficients minimum distortions was achieved.

D. Data hiding in 3d objects

P.Amat et al (2010) Proposed a data hiding method in 3D objects based on minimum spanning tree (MST) . The research work of this paper was finding and synchronizing the particular areas of 3D object for embedding the secret message. By changing the connectivity of edges in the selected area composed of quadruples. This method was blind and lossless. The unique feature

in this method is position of the vertices in the 3D objects never change. Texture and color of the object 3D logo can also be embedded using the method.

E. Data Hiding In Flash Video

Jason Paul Cruz and Gregory Tangonan Described about data hiding in Flash Video(FLV).Steganographic protocol is used to hide the data, with the existing methods hiding the stegofile at the end of the video tag is recommended. In this method minimum distortions were found and looked like original FLV file , one stegofile is hidden inside the FLV and not at the end of the File or header . Stegofile cannot be altered by attackers even after coverting it into different file format.

F. Audio steganography .

Y.F. Huang et al (2010) presented a algorithm for embedding the data in the inactive frames which is used in Voice over Internet Protocol(VoIP).High embedding capacity is achieved by using inactive frames encoded by G.723.1 codec with 6.3 kbps than the active audio frames. In general Hangover algorithm is used for detecting inactive voices .Improved Voice Activity Algorithm (VAD) called residual energy method is used.

G. Network steganography

Jozef Lubacz et al (2014) reviewed important principals of network steganography and also discussed about classification and techniques used for network steganography. Network Steganogrpahy was classified based on the protocol functions which are associated with OSI layers and based on the modification of Protocol Data Units (PDU).

Jorge Blasco et al (2011) discussed about the problems of using steganography through a network protocol called Hyper Text Transfer Protocol (HTTP). Studies shows that most of the inside malicious employees steal the confidential information from their organizations. Authors contributed a framework called Stego-Proxy which limits usage of HTTP for secret communications using covert channels .

Chuan Qin et al (2012) presented a reversible steganographic method using histogram shifting mechanism. Reference pixels were selected according to the distribution characteristics of image content , then image in painting scheme was used to generate a prediction image which is identical in structure and geometric information of the cover image .The histogram of the prediction error was shifted to embed the secret message bits .From the smooth region fewer reference pixels were chosen and from the complex region more reference pixels were chosen .

Shouchao song et al (2011) proposed new protocol for secret communication by combining steganography anf cryptography . Boolean functions were used for encryption and increment and decrement of LSB .Authors focused on grayscale images . Encryption and data hiding were done at same time unlike traditional methods, so less computation time and optimal embedding ratio was achieved. The receiver does not require original cover image to restore the secret information.

H. Data hiding in ECG signal.

Ayman Ibaida and Ibrahim Khalil (2013) provided method of hiding patient confidential data using the ECG signal. Five level Discrete wavelet transformation and scrambling matrix was applied to find the correct embedding sequence. This method was being used in remote patient monitoring systems in hospitals. Point –of-care(PoC) technologies have becoming popular that provides reliable transformations of patient medical information to doctors in emergency .Patient Confidential information was encrypted first and then wavelet decomposition was applied for embedding the data.

I. Review On Saliency

Visual saliency is the process of finding important region in an image . Chirag Agarwal et al (2013) proposed a data hiding method using DWT based on saliency model, they proposed a algorithm which hides the data into visually interested areas such as host image. Visual attention model is used to find suitable interested areas in an host image.

Hao bin et al (2011) stated that information can be embedded in the optimal component of the motion vectors with large amplitude. they used matrix encoding technique for decreasing the modification rate of motion vector. since they used phase angle to embed the data they claimed that video quality is high.

The authors Changyong Xu and Xijian Pingin focused on the motion component which is obtained by difference between the adjacent frames for embedding the secret message, after calculating the motion component , two level wavelet decomposition was done then secret message was embedded in the low frequency coefficients which has large moving speed. Uncompressed

video sequence was used and they extracted secret bits even after encoding.

Feng Pan et al (2010) reveals that the data bits of the secret message are embedded in motion vectors of H.264 video. The authors used linear block codes for reducing the modification rate of motion vectors. They claimed that this method has large embedding capacity, imperceptibility and good video quality as well.

Yun Cao et al (2012) described Steganalysis methods which were focused on identifying secret messages that were embedded by using motion vector based methods. The authors concentrated on the methods which used non optimal selection rule for choosing motion vector. These steganalysis methods are different from conventional steganographic methods used in spatial/transform domain. Results proved that these features were sensitive to Exploiting MV reversion and detected motion vectors based steganography in the low embedding rates also.

Saliency detection is normally based on the assorted features like color, intensity, orientations texture, and motion. According to human visual system motion information plays vital role in video sequence, by means of motion vector spatiotemporal saliency algorithm is proposed earlier .In that work authors combined the Block matching algorithm and optical flow method for calculating motion estimation. Yaping Zhu et al (2011) used "SUN (Saliency Using Natural Statistics) model to measure the saliency obtained from natural sequences, by combining the temporal saliency obtained by motion vector and spatial saliency by SUN model new spatiotemporal saliency map was proposed.

Data could be hided in H.264 encoded video. In this method data is hidden in the inter prediction stage using their different block sizes of H.264 encoder. The authors described that original secret message could be extracted without original host video. Inter prediction process is used to hide the data in which motion estimation is the important process of finding the macroblock. Motion estimation is applied to different block types of H.264.This algorithm makes decision in selecting the frame for hiding purpose,then it performs motion estimation based on the macroblock candidates and ensuing the high capacity.

1) Steganography in Images: When hiding information inside images the LSB (Least Significant Byte) method is usually used.To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of. Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion. It is important to remember that if you hide information inside of an image file and that file is converted to another image format, it is most likely the hidden information inside will be lost.

2) Steganography in Audio: When hiding information inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. Spread Spectrum is another method used to conceal information inside of an audio file. This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum. Echo data hiding is yet another method of hiding information inside an audio file. This method uses the echoes in sound files in order to try and hide information. By simply adding extra sound to an echo inside an audio file, information can be concealed. The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file.

3) Steganography In Video: When information is hidden inside video the program or person hiding the information will usually use the Discrete Cosine Transform method.DCT works by slightly changing the each of the images in the video, only so much though so it's isn't noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up. For example if part of an image has a value of 6.667 it will round it up to 7. Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video. When only a small amount of information is hidden inside of video it generally isn't noticeable at all, however the more information that is hidden the more noticeable it will become.

J. Concluding Remarks

The major techniques like adaptive steganography, DCT, DWT are less prone to attacks but having less capacity when compares to spatial domains. Data hiding could be done by pixel value differential method, 3D objects, Flash Video , Electro Cardio Gram (ECG) signal can be used as carrier file to do steganography. Visual saliency is the process of finding important

region in an image. Research is focused on how to avoid the illegal copies or piracy. Cryptography, watermarking, and steganography are the data hiding techniques that are mainly used for this purpose. Cryptography may attract the attention of interceptors so data hiding techniques evolved. Digital watermarking is used for copyright protection whereas steganography is used for covert communications. Extensive research has been carried out by combining cryptography and steganography

III. PROPOSED VIDEO STEGANOGRAPHY USING DWT BASED ON MOTION SALIENCY MODEL

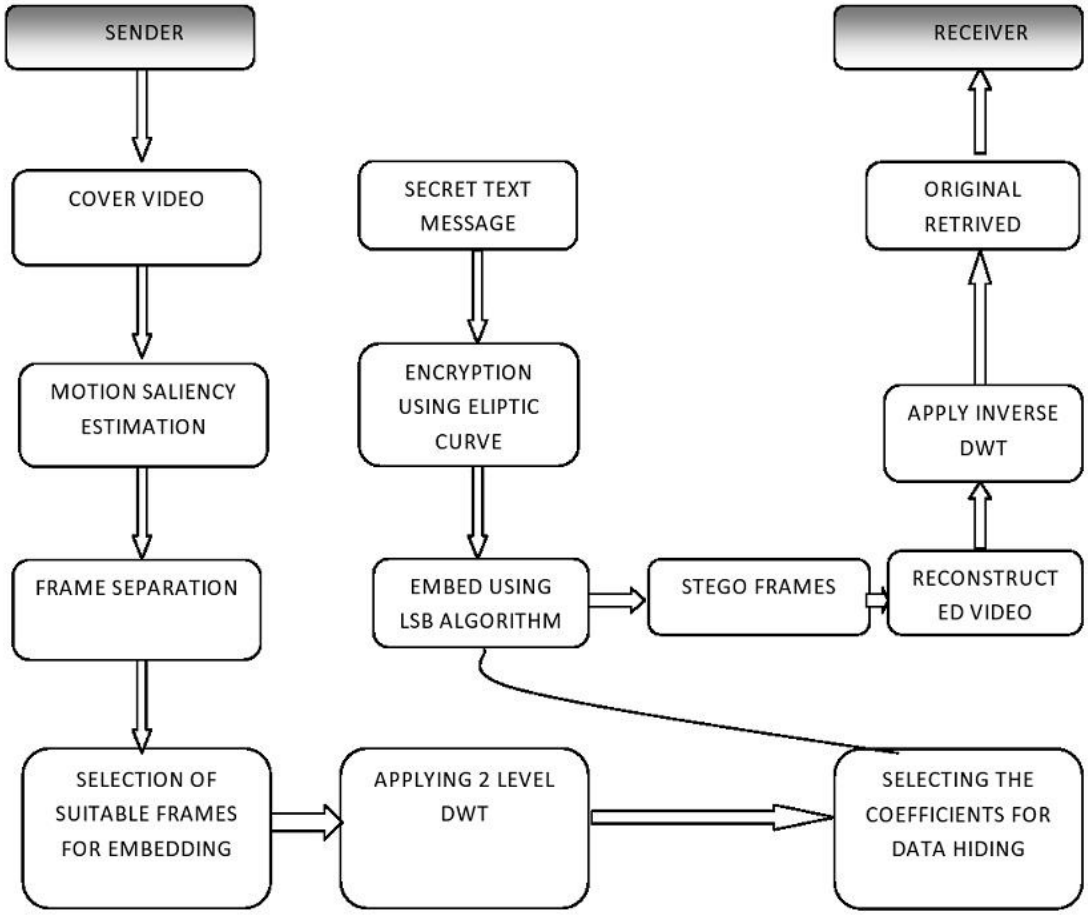


Fig 1 : Proposed System Architecture for Stegnography model

Steganography is the process of concealing the message inside any multimedia carrier. The proposed method as depicted in figure 1 embeds the secret text message using the Discrete wavelet transform and Singular wavelet decomposition . Here video is taken a carrier file and motion saliency is calculated based on Itti Koch (3) method . The temporal frames are decomposed into four sub bands namely LL,LH,HL and HH . The LL sub band is selected for steganogrphy and then SVD is applied in that particular frame , after that using the LSB replacement algorithm secret message is embedded in the SVD portion. After embedding combine all the sub bands to reconstruct the original video without any distortion .By applying the inverse DWT the original secret message was extracted without any loss of information .

IV. EXPERIMENTAL RESULTS

The Proposed algorithm is tested and evaluated using MATLAB 2014b Version . figure 2 shows the user getting input message to hide and figure 3 shows the motion saliency . The frames are selected for steganography for as per figure 4 and further decomposed into four sub bands after applying DWT. SVD portion is selected then message is embedded using LSB algorithm.

PSNR and Noise Correlation (NC) results in figure 6 proved that the impercebility of the proposed method .

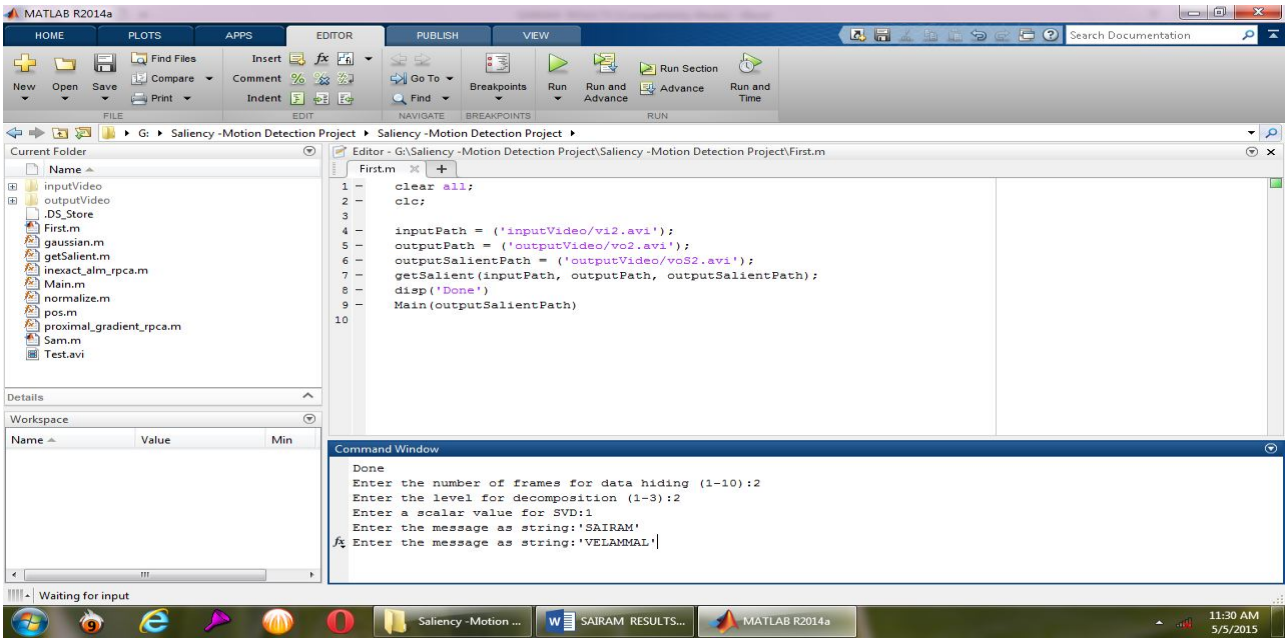


Fig 2: Getting input from the user for the secret message to hide

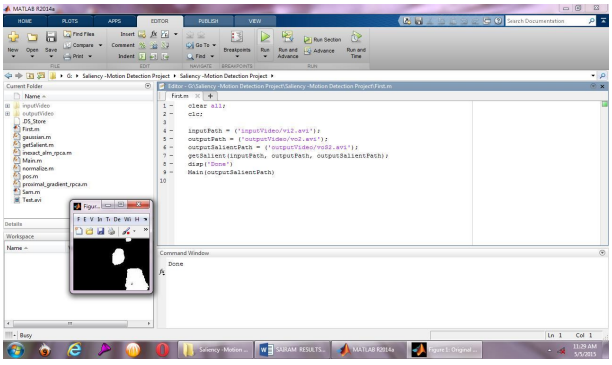


Fig 3: Motion Saliency of the video

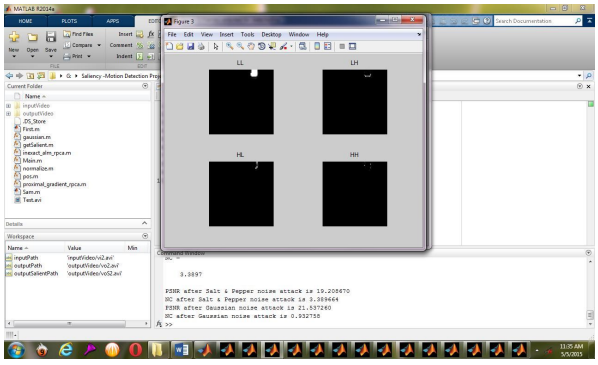


Fig 4: DWT to the frame selected for data hiding

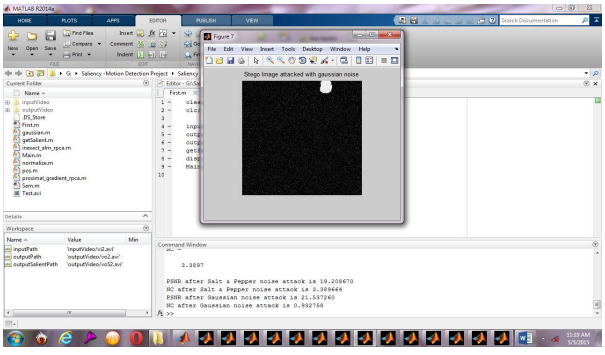


Fig 5: Stego image attacked with gauissian noise .

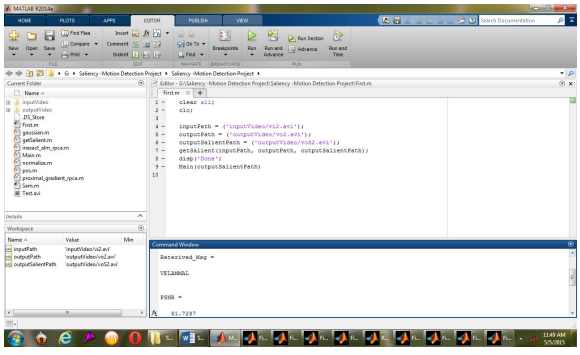


Fig 6: Retrived original message with out any loss

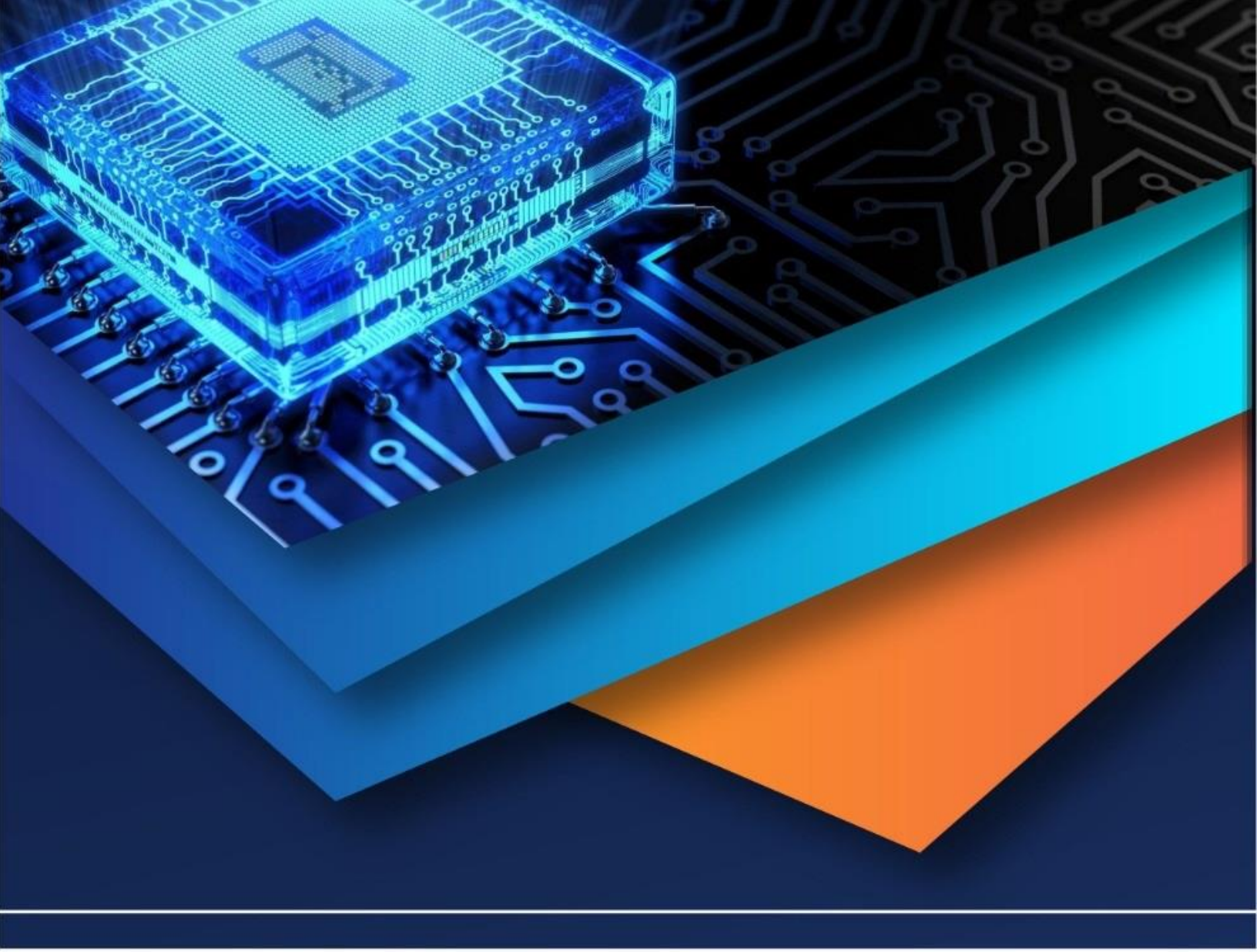
The robustness is evaluated by adding Gaussian noise and salt and pepper noise as in figure 5. The results proved that secret image is not altered after attacks and retrieved without any loss as per figure 6

V. CONCLUDING REMARKS

In this study of various literature reviews and effective methods of steganography algorithms have their own merits and demerits. In the introduction section it was able to understand various spatial and frequency domains which are used for data hiding. From the Chapter 2 Literature review as proposed by some authors watermarking is one of the multimedia security techniques which differ from sreganography by its goal. The major techniques like adaptive steganography, DCT, DWT are less prone to attacks but having less capacity when compares to spatial domains. Data hiding could be done by pixel value differential method, 3D objects, Flash Video , ECG signal can be used as carrier file to do steganography. Visual saliency is the process of finding important region in an image . Motion Vectors can be detected by Saliency. Steganography technique is widely used to covert communication in various fields like military , bank transactions, health information system , government's confidential transactions and to carry out business secrets. We propose a new steganographic model by using DWT and Motion saliency that is depicted in the architectural diagram

REFERENCES

[1] Jorge Blasco, Julio Cesar Hernandez-Castro, Jose´ Marı´a de Fuentes, Benjamı´n Ramos, A framework for avoiding steganography usage over HTTP – Journal of Network and Computer Applications. Elsevier Ltd. doi:10.1016/j.jnca.2011.10.003(2011)
[2] Shouchao Song , Jie Zhang, Xin Liao, Jiao Du, Qiaoyan Wen, A Novel Secure Communication Protocol Combining Steganography and Cryptography , Procedia Engineering -pp 2767-2772 Elsevier .doi:10.1016/j.proeng.2011.08.521(2011)
[3] Abbas Cheddad, JoanCondell, KevinCurran, Paul Mc Kevitt, Digital image steganography:Survey and analysis of current methods .Signal Processing Elsevier. doi:10.1016/j.sigpro.2009.08.010(2009)
[4] Nan-I Wu, Kuo-Chen Wu, Chung-Ming Wang- Exploring pixel-value differencing and base decomposition for low distortion data embedding-Applied Soft Computing .Elsevier doi:10.1016/j.asoc.2011.09.002(2011)
[5] P.Amat,W.Puech , S.Druon , J.P.Pedeboy –Lossless 3D steganography based on MST and connectivity modification –Signal Processing :Image Communication. Elsevier ved. doi:10.1016/j.image.2010.05.002(2010)
[6] Der-Chyuan Lou ,Chen-HaoHu LSB -Steganographic method based on reversible histogram transformation function for resisting statistical steganalysis. Information Sciences.Elsevier.doi:10.1016/j.ins.2011.06.003(2011)
[7] Min-Jeong Lee, Kyung-Su Kim, and Heung-Kyu LeeDigital - Digital Cinema Watermarking for Estimating the Position of the Pirate Object Identifier 10.1109/TMM.2010.2061221NOVEMBER (2010)
[8] Jason Paul Cruz, Nathaniel Joseph Libatique, and Gregory Tangonan ," Steganography and Data Hiding" in Flash Video (FLV)
[9] Y. F. Huang, Shanyu Tang, and Jian Yuan -Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec , *IEEE* Copyright (c) 2010 IEEE.
[10] Chuan Qin, Chin-Chen Chang, Ying-Hsuan Huang, and Li-Ting Liao- An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting .IEEE transactions on circuits and Systems for Video Technology .Vol 23, No. 7 Mechanism --Digital Object Identifier 10.1109/TCSVT.2012.2224052(2013)
[11] Józef Lubacz, Wojciech Mazurczyk, and Krzysztof Szczypiorski , Principles and Overview of Network Steganography-- --IEEE Communications Magazine , May (2014)
[12] Linjie Guo, Jiangqun Ni, and Yun Qing Shi, Uniform Embedding for Efficient JPEG Steganography ,IEEE Transactions On Information Forensics And Security, Vol. 9, No. 5, May 2014--Digital Object Identifier 10.1109/TIFS.2014.2312817 (2014)
[13] Ayman Ibaida and Ibrahim Khalil--Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems, IEEE Transactions On Biomedical Engineering, Vol. 60, No. 12, December (2013)
[14] Chirag Agarwal, Arindam Bose, Somnath Maiti, Nurul Islam, Subir Kumar Sarkar ,Enhanced Data Hiding Method Using DWT Based on Saliency Model, IEEE Conference .D.O.I 10.1109/ISPCC.2013 (2013)
[15] Hao-Bin ,Zhao Li-Yi, Zhong Wei-Dong ,A Novel Steganography Algorithm Based on Motion Vector and Matrix Encoding, IEEE Conference. D.O.I 10.1109/ ICCSN.2011.6013622 (2011)
[16] Changyong Xu, Xijian Ping, A Steganographic Algorithm in Uncompressed Video Sequence Based on Difference between Adjacent Frames, IEEE Conference D.O.I:10.1109/ICIG.2007.36(2007)
[17] Feng Pan, Li Xiang , Xiao-Yuan Yang, Yao Guo , Video Steganography using Motion Vector and Linear Block Codes .IEEE Conference .D.O.I 10.1109/ICESS.2010.5552283.(2010)
[18] Yun Cao, Xianfeng Zhao,Dengguo Feng , Video Steganalysis Exploiting motion Vector Reversion-Based Features. IEEE Signal Processing Society .D.O.I:10.1109/LSP.2011.2176116(2011)
[19] Yaping Zhu, Natan Jacabson, Hong Pan, and Truong Nguyen, Motion-Decision Based Spatiotemporal Saliency for Video Sequences. IEEE Magazine (2011)
[20] Mohammad Ali Akhaee, S.Mohammad Ebrahim Sahraeian,Baluet SAnkur, Farokh Marvasti , Robust Scaling Based Image Watermarking Using Maximum Likelihood Decoder with Optimal Strength Factor, IEEE Transactions on Multimedia , Vol 11, No 5, August(2009)
[21] Min-Jeong Lee, Kyung-Su Kim, and Heung-Kyu Lee, Digital cinema watermarking for estimating the position of the pirate., IEEE transactions on Multimedia , Vol 12, No 7 November (2010).D.O.I 10.1109/TMM.2010.2061221.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY