ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 1, April 2013

Echo Hiding Approach in Video Forensic

Dr. A.K.Sen[1], Susmita Dutta[2], Sanjay Dabadgaonkar[3]

Principal, ST. Francis Institute of Technology, S.V.P Road MT. Poinsur, Borivali(W), Mumbai- 400 103, India[1]

Assistant Professor, Electronics & Telecommunication Engineering Department, ST. Francis Institute of Technology, S.V.P Road MT. Poinsur, Borivali (W), Mumbai- 400 103, India[2]

Area Chair, Electrical & Electronics Engineering Department, Tolani Maritime Institute, Induri, Talegaon-Chakan Road, Pune - 410 507, India[3]

Abstract: With the advancement in the information processing and transferring device, security of the transferred information is of significant concern. Several methods have been developed for secured data transfer. Steganography is one of the methods. Our invention relates to Digital steganography, which is the art of inconspicuously embedding data within a data. Steganography's goal in general is to hide data well enough that unintended recipients do not suspect the steganographic medium of containing hidden data. Here, in this article we introduce this steganographic technique that hides messages in video as well as audio which proposes a scheme that improves the robustness of data hiding. In Echo hiding, message is embedded in a sound signal in video stenography by introducing an echo into the discrete signal. It has the advantage of high data rate. In echo hiding, encoding is done by breaking the signal into blocks & each block is assigned binary "1" & binary "0" depending upon some offset value that we use in encoding.

Keywords: Audio steganography, video steganography, Echo hiding, Discrete cosine transform.

I. INTRODUCTION

Steganography is the science of hiding information whereas the goal of cryptography is to make data unreadable by a third party. There are a large number of steganographic methods that most of us are familiar with (especially if we watch a lot of spy movies!), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding information, such as:

• Covert channels (e.g., Loki and some distributed denial-of-service tools use the Internet Control Message Protocol, or ICMP, as the communications channel between the "bad guy" and a compromised system)

• Hidden text within Web pages

• Hiding files in "plain sight" (e.g., what better place to "hide" a file than with an important sounding name in the c:\winnt\system32 directory?)

• Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in and of itself) and then decrypt it. There are a number of uses for steganography besides the mere novelty. Stego can also be used to allow communication within an underground community. There are several reports, for example, of persecuted religious minorities using steganography to embed messages for the group within images that are posted to known Web sites.

II. VIDEO FORENSIC

An Video forensic means steganography in video**.** By developing the computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the covert exchange of information. The method of video steganography is among the methods that has received very little attention in recent years compared

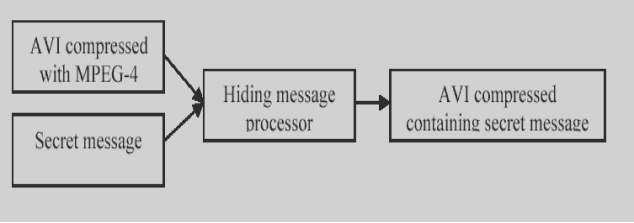

Fig.1 Model for Steganography Approach

to audio and image steganography. In addition to being used in the covert exchange of information, steganography is used in other grounds such as copyright, preventing e-document forging, etc.

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 1, April 2013

A. *How it works*

Video files are generally consists of images and sounds, so most of the relevant techniques for hiding data into images and audio are also applicable to video media. In the case of Video steganography sender sends the secret message to the recipient using a video sequence as cover media. Optional secret key 'K' can also be used during embedding the secret message to the cover media to produce 'Stego-video'. After that the Stego-video is communicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with the extracting algorithm to extract the secret message from the Stego object. The original cover video consists of frames represented by Ck (m,n) where 1 £ k £ N. 'N' is the total number of frame and m,n are the row and column indices of the pixels, respectively. The binary secret message denoted by Mk(m, n) is embedded into the cover video media by modulating it into a signal. Mk(m, n) is defined over the same domain as the host Ck(m,n).The Stego-video signal is represented by the equation Sk(m, n) = Ck(m, n)+ak (m, n) Mk(m, n) , k = 1, 2, 3 ... . .N

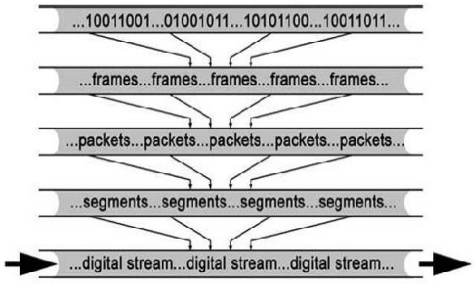

Fig.2 Frames of video

Where ak (m, n) is a scaling factor. For simplicity ak (m, n) can be considered to be constant over all the pixels and frames. So the equation becomes: Sk(m, n) = Ck(m, n)+a (m, n) Mk(m, n) , k = 1, 2, 3 . . .N. When working with a video signal, series of binary bits that are sent out as one continuous stream of digital data called as digital stream, which is in the form of zeros and ones, which are grouped into elements called frames. Groups of frames are organized into packets. Groups of packets are organized into segments. The result of a group of segments is the digital stream.

A. *Description*

a. In our project, video is accessed and complete information about it is extracted
b. The file to be hidden is then accessed and the no. of bytes in it are calculated.
c. Every frame of the video is broken up into blocks of 8x8 bits.
d. The block is then compressed using Discrete Cosine Transform. and two block coefficients are chosen for all further reference.
e. Dk1= [2 3] , Dk2=[4 1]
f. The block is further converted into YUV colour model.
g. Based on whether bits in the file to be hidden are '0 or'1', the 2 coefficients' or their positions are manipulated.
h. For every bit in the file to be hidden, one 8x8 block is accessed and a pattern is set in it manipulating Dk1 and Dk2.
i The above process is then reversed and the block is replaced into the frame.
j. The process continues till all the bits of the file are accessed.
k. In the above process, if all blocks of a frame are utilized the next frame is accessed.
m. Similarly while retrieving the file to be hidden, the pattern present in each 8x8 block of a frame is studied and accordingly bit '0' or '1' is extracted.

III. ECHO HIDING

All In the Echo hiding procedure, the message which has to be hidden is embedded into the Original audio signal. Then it is sent to the receiver. In order to encode, an echo signal is generated from the original audio signal. To hide data successfully, three parameters of echo are varied- a) Amplitude, 2) Decay rate & 3) Offset (delay time) from the original signal. All the parameters are set below the human hearing threshold so that echo is not easily resolved. One offset value represents binary "one", & other offset value represents binary "zero". Now in the first method, only one echo signal is generated from the original message signal. So the information that will be encoded is of only one bit. The original audio signal is broken down into blocks at the start of encoding process. Each block is assigned binary "zero" or binary "one" based on the secret message. At the transmitter side the original signal. is first echoed and then the secret message is embedded into the signal. This signal is than fed to the mixer, thereafter it is given to the encoder. Two mixers are used here so as there is no intermixing of 0's and 1's.The output from the mixer is fed to the encoder.

A. Description of the invention

Echo data hiding embeds a data value in an analog or digital host audio signal by introducing one or more echoes, or resonances, offset in time from the host audio signal by an offset value associated with the data value of the bit. The alteration to the host signal can be characterized in term of several parameters: the number of echoes introduces; the offset value separating in the first echo from the host signal and echo from one another, and the amplitudes of the echoes. For sufficiently small values of these parameters, the HAS interprets an added resonance. Echo hiding introduces resonance to the host signal which are on the order of human vocal track resonances and are generally perceived as natural and considered enhancements rather than noise. The embedded data is resistant to removal by many of the known loss data compression algorithm.

IV. PROPOSED SYSTEM

Basically audio file and moving image makes a video file. In our method the secret message is embedded into cover audio signal as an echo. Three parameters of the echo of

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 1, April 2013

the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary message. They are set below to the threshold of Human Auditory System (HAS) so that echo can't be easily resolved. Echo hiding schemes are paid more attention because they do not need the original audio for detection. Especially, echo hidings considered to be better in terms of imperceptibility since it just adds delayed.

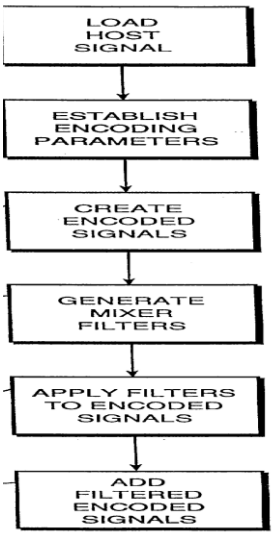

Fig.3 Model of the system

in order to encode a string of several bits, a single bit is encoded into each of several temporal segments of signal. A signal such as the host audio signal 200 shown in fig is divided into segments 205.each of which is then processed as an independent host audio signal to introduce an echo embedding the bit desired value for corresponding position in the string.

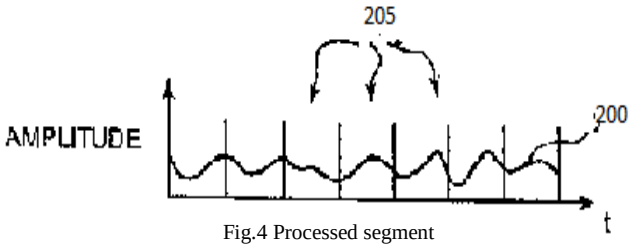

Fig.4 Processed segment

The processed segments are combined to constitute an encoded string signal. The fig. 5 shows the host audio signal 200 with a zero echo 209 embedded in the other of the encoded signals by processing with a zero function. The encoded string signal containing the desired sequence of bits is created by arranging segment of the encoded signal to constitute a signal.

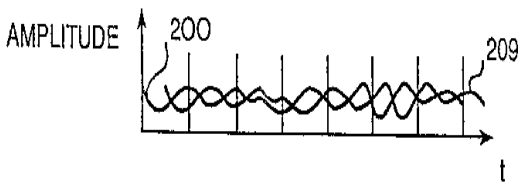

Fig.5 Host Signal with echo signal

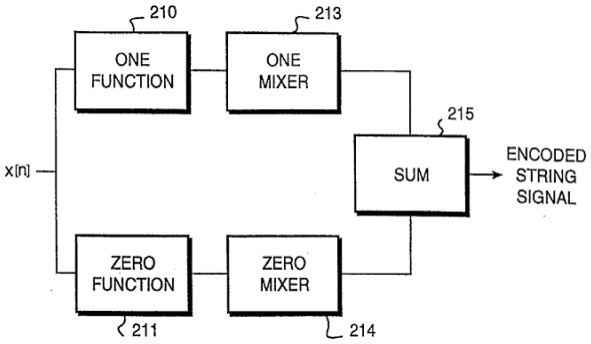

Fig.6 Model of proposed system

The fig.6 shows the process beginning with the host audio signal x[n], which is processed by both the one function, at 210, and the zero function, at 211, to create encoded signal. Each encoded signal is filtered by one mixer filter, at 213,or the zero mixer filter at 214,and the results are summed at 215 to from the encoded signal. The fig.7 show a one mixer filter 216 and zero mixer filter a zero mixer filter 218 for filtering the encoded signals created by processing the host audio signal 200 with the one function and the zero function, respectively, to create an encoded string signals created by processing the host audio signal containing the series of bit values 220 in the corresponding segments 205, shown in fig.7.

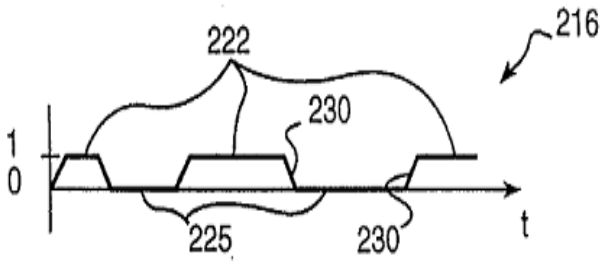

Fig.7 Mixing with echo signal

The information-hiding process in a steganographic system starts by identifying a video's redundant bits (those that can be modified without destroying that video's integrity).

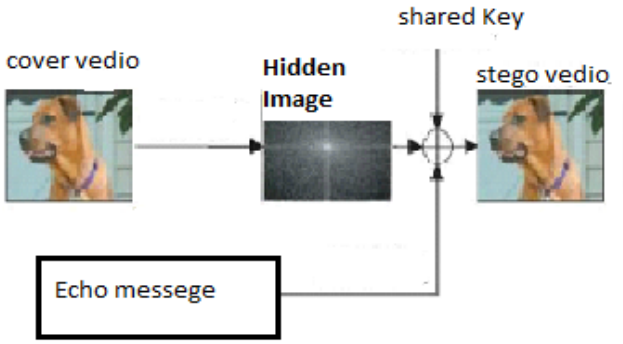

Fig.8 Output of the system

The embedding process creates a Stego medium by replacing these redundant bits with data from the hidden message. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Steganographic communication senders and

receivers agree on a steganographic system and a shared secret key that determines how a message is encoded in the cover medium.

CONCLUSION

A new approach is proposed to resolve two problems of substitution technique of audio steganography. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness.

REFERENCES

[1] Authentication of secret information in image Steganography Babu, K.S.; Raja, K.B.; Kiran, K.K.; Manjula Devi, T.H.; Venugopal, K.R.; Patnaik, L.M.

[2] IEEE Transactions on computers Volume 58, Issue 5, May 2009 Page(s):662 - 676 Provably Secure Steganography Hopper, N.; von Ahn, L.; Langford, J.; S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok.

[3] Steganography and steganalysis-robert krenn,internet publication,march 2004 http://www.kkrenn.nl/univ/cry/steg/article.pdf.

[4] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in Proc. 6th Int. Workshop on Information Hiding, Toronto, Canada, 2004, pp.128– 147.

[5] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces re-sampling," IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 758–767, 2005.

[6] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Trans. Signal Processing, vol. 53, no. 10, pp. 3948–3959, 2005.

[7] S. Prasad and K. R. Ramakrishnan, "On resampling detection and its application to image tampering," in Proc. IEEE Int. Conf. Multimedia and Exposition, Toronto, Canada, 2006, pp. 1325–1328.

[8] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromaticaberration," in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006, pp. 48–55.

[9] M. K. Johnson and H. Farid, "Metric measurements on a plane from a single image," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006-579, 2006.

[10] M. K. Johnson and H. Farid, "Detecting photographic composites of people,"in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China, 2007.

[11] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inform. Forensics Security, vol. 3, no. 2, pp. 450–461, 2007.

[12] M. K. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in Proc. 9th Int. Workshop on Information Hiding, Saint Malo, France, 2007, pp. 311–325.

[13] Methods of Audio Steganography, Internet Publication on http://www.snotmonkey.com/work/school/405/methods.html

BIOGRAPHY

Dr. Asim Kumar Sen, Presently Working as a Principal and Professor, Saint Francis Institute of Technology, Borivali, Mumbai. Completed Ph.D. in 1995 from IIT Kharagpur. MIE (India), LM of International Society for Reliability Engineers (India Chapter), LMISTE, Fellow of IETE, Honorary Council Member of Flash India Management Senate, Mumbai, Referee of the Journals published by A.M.S.E, France, Chartered Engineer, LM of Indian Nuclear Society, Experienced faculty in the field of Electronics, Instrumentation and control, Digital Signal Processing, Industrial Engineering and Management. Having administrative experience as a Principal. About 70 Publications in International / National Journals and Conference Proceedings. Guided several Projects and Ph. D. Thesis and in the panel of Supervisor for various Universities for guiding research related activities.

Prof. Susmita Dutta, presently working as Assistant Professor, Electronics & Telecommunication Engineering Department, Saint Francis Institute of Technology, Borivali (W), Mumbai. She has completed B.E. (Electrical Engineering) and Post Graduation i.e. M.Tech (ROBOTICS). She is having total experience of about 5 years, which includes three years and six months of teaching and eight months of industry experience. She has published two papers one each in national and international conference and presented two papers in national and international conference. She is having professional memberships of ISTE, ICN.

Prof. Sanjay Dabadgaonkar, Presently working as a Area Chair, Department of Electrical and Electronics and Senior Associate Professor in Tolani Maritime Institute, Induri, Pune. Total Teaching experience of about 23 years. Worked as a Head of Dept. in Electronics and Telecommunication at College of Engineering under Dr B A M U Aurangabad. Published 6 Papers in international Journals and Presented 45 papers in International / National Conferences. Attended several workshops, Honored with a Best teaching faculty award, Member of University LIC and Chairman / Head during NBA & AICTE Visit in COEO, Organised Two National Level conferences. Session Chair for national & international conference, Fellow member of IETE, ISTE, IE. Research (Ph.D) in Simulation of Power Electronic systems for onboard ship is in progress.