Data Hiding in Video using Inverse Improved LSB and Secrete Key

Pranjal K. Kshatriya[1] Jyoti B. Bhand[2] Sujata L. Kakade[3] Prof. R. R. Rathod[4]
[1,2,3]BE Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]SGOI College of Engineering, Belhe, SPPU Pune

Abstract— Emergence of internet has caused it to be possible to transfer the information in one place to some other place rapidly and accurately. This data when undergoes the web could become a victim of the hackers who is able to steal, modify and misuse the information. So it will be required to transfer the data with utmost security. Steganography is one particular solution to the problem. Random frame selection, pixel swapping and encryption of message has been done to improve the security of the key information which goes beneath the cover of video clips. The strategy can also be able to allow for massive amount of data in video.

Key words: Steganography, LSB, Discrete Cosine Transform, Cryptography

I. INTRODUCTION

In 90's, the emergence of internet in throughout the world has generated a drastic change in the people's life style. With the advancement of internet and information revolution, shopping, rail reservation and even money transfer is now online i.e. people do not need to go anywhere to obtain each one of these above job done instead they have the ability to make every one of these job done even yet in sitting within their respective home. Besides these, the emergence of social site like twitter, wat's up and Facebook has made all individuals to be {in touch with each other 24/7 hours People are actually able to exchange the data with one another very rapidly and promptly. Interchanging the data online has begun creating problems of intercepting this information by some unauthorized, unsocial band of people famously called hackers. So this can be a need of the hour to style or develop some sort of application which is often able make sage and secure transfer of utmost important or valuable information without having to be acknowledged by the unauthorized person. The perfect solution is with this problem is based on two most trusted techniques i.e. Cryptography and Steganography. Steganography is one of many techniques which was created to fight with such kind of problems. Steganography is actually application which will be developed for hiding the valuable or confidential data in an address file in this way that no an added when compared to an authorized person knows the presence of such hidden information in cover file. Audio, Video Text as well as image can be utilized as an address file In steganography the key or confidential information is hidden in an innocent cover file in this way that nobody may also suppose that such sort of information is hidden within the cover file which might be any image, audio or video. Embedding payload and embedding efficiency are both crucial parameters of any steganography system. Number of data which is often hidden in the cover file is recognized as the embedding payload. The ability of steganography system to cover up the maximum amount of data as it can certainly with inducing as least distortion as it could on the cover file is called the embedding efficiency. High embedding efficiency could be the prime requirement of any steganography system. High embedding efficiency means least distortion in the cover file and hence it is extremely tough to assume an existence of any secret information in the cover file. This helps it be difficult to utilize any stage analysis tool to extract out the data from the cover file. Embedding efficiency and embedding payload are often enjoying inverse proportional relationship. Increasing the embedding efficiency will decrease the embedding payload and vice versa

II. LITERATURE SURVEY

In 2011 Ming, suggested a steganographic method for hiding large amount of data. Discrete Cosine Transform is used in this with this process. Its main objective is increasing the payload while keeping the robustness and simplicity intact. In this technique, Discrete Cosine Transform coefficients of I-frames are computed and then secret information get encrypted by performing modulation between quantized DCT coefficients and secret information [1]. In 2008 Chen, present a reversible data hiding scheme centered on histogram modification. We exploit a binary tree structure to resolve the problem of communicating pairs of peak points. Distribution of pixel differences can be used to attain large hiding capacity while keeping the distortion low [2]. In 2011, WeiWei and some researcher proposed a steganography method for wavelet compressed video. In this paper, steganography method for compressed video is presented. Here is the easiest method to send large amount of secret data. Firstly, video data get compressed using wavelet after that bit plane complexity segmentation steganography is used for encryption of secret data. In this approach DWT transformed video is quantized to somewhat plane structure and then BPSC algorithm is put on the video in wavelet domain. This technique is get tested for 3-D SPIHT-BPSC steganography and JPEG 2000-BPSC [3]. In 2012, Yuan proposed a steganography algorithm for AVI (Audio-Video Interleaved) file standard using swapping method. We can do the comparative analysis of JPEG image steganography and Audio video interleaved (AVI) steganography has been accomplished regarding quality and size get. Author implies that by using UTF-32 encoding in the swapping algorithm will increase the strength of the important thing and also the security with this steganography system. Among its disadvantage is its low payload capacity [4]. In 2003, Lu in his paper presented an invertible data hiding approaches for compressed video. This scheme is good for Motion Picture Expart Group (MPEG) standard. In this approach, hidden embedded data of the video could be decrypted without the necessity of copy of original MPEG video and covert video. This scheme used only in frequency domain. Low complexity and low visual distortion is the key points of this approach while low payload capacity is the drawback with this method [5]. In 1999, Chae and his fellow researchers presented a steganography model for hiding the presence of secret information in a cover video of any format.

In this model colored video file get pixel-wise manipulated to insert a secret data. Firstly, this approach does the segmentation of the trick information right into a blocks before embedding it in to the cover video. In the next level, this approach embeding these block in to the pseudo random location in video file. Location for embedding is done by re-ordering the trick key that will be shared by both sender and receiver [6].

III. OVERVIEW OF STEGANOGRAPHY SYSTEM

Steganography is the process of hiding the information in some other medium like image, audio and video. From ancient time steganography get used by people. In past years, secret information is hidden behind the wax, scalp of the slaves, in rabbits etc. After some timespan, the application of steganography and its area has become widened. After introduction of digitization era, digital steganography has become as the new tool to hide the information secretly. Text, digital image, digital audio and digital video has become the sub parts for data hiding. Some of the technique which are necessary to understand steganography technique,

A. Cover Media

It is the medium for encryption of data in which secret information is get encrypted in such a way that it is difficult to detect that data is present or not.

B. Stego- Media

It is medium obtained after encryption of secret information. Secret data- The data or information is get hidden in cover media.

C. Steganalysis

It is the process of detecting, presence of secret data in cover media.

1) *Video Steganography:*

Video is just a digital medium for the recording, copying and broadcasting of moving visual images. The utmost effective technique is that to hide secret message without affecting the caliber of video, structure and content of video. After hiding a secret data in video create "stego "video file that will be send to the receiver.

IV. PROBLEM STATEMENT

The former contains linguistic or language kinds of hidden writing. The later, such as for instance invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to really have a good understanding of linguist. Recently, everything is trending toward digitization. And with the development of the web technology, digital media may be transmitted conveniently within the network. Therefore, messages may be secretly carried by digital media utilizing the steganography techniques, and then be transmitted through the web rapidly. A variety carrier file formats can be utilized to cover up the images or some other files, but digital images are typically the most popular due to their frequency on the internet.

V. EXISTING SYSTEM

In existing system investigated adaptive mechanisms for high-volume transform-domain data hiding in MPEG-2 video which is often tuned to sustain varying degrees of compression attacks. The information is hidden in the uncompressed domain by scalar quantization index modulation (QIM) [7] on a selected pair of low-frequency discrete cosine transform (DCT) coefficients. It proposes an adaptive hiding scheme where in fact the embedding rate is varied in accordance with the sort of frame and the reference quantization parameter (decided based on MPEG-2 rate control scheme) for that frame. For a 1.5 Mbps video and a frame- rate of 25 frames/sec, it is to embed almost 7500 bits/sec. Also, the adaptive scheme hides 20% more data and incurs considerably less frame errors (frames for that the embedded data isn't fully recovered) compared to the non-adaptive scheme

VI. PROPOSED SYSTEM

In this paper, information security utilizing information concealing audio video steganography with the help of PC measurable strategies gives better concealing limit we have got an attempt at concealing picture and content behind video and audio document and separated from an AVI record utilizing 4 minimum noteworthy piece insertion technique for video steganography and stage coding audio steganography. Steganography could be the technique for concealing any mystery data like watchword, content and picture, audio behind unique spread record. Unique message is changed over into figure content by utilizing mystery key and from then on covered up to the LSB of unique picture. The proposed framework gives audio-video cryptostegnography which can be the mixture of picture steganography and audio steganography utilizing Forensics Technique being an instrument to validation. The principal point is always to shroud mystery data behind picture and audio of video record. As video is the utilization of numerous still casings of pictures and audio, we are able to choose any casing of video and audio for concealing our mystery information. Suitable algorithm, like, AES is utilized for picture steganography suitable parameter of security and confirmation, thus information security could be expanded. Also, for information implanting we utilize 4LSB algorithm. The robustness of the watermark embedded utilizing the LSB coding method, increases with increase of the LSB depth is employed for data hiding.

A. Advantages

- Quality of video file is strictly preserved even with secret data embedding.
- Ability to encrypt and decrypt the information with the images.
- With this method, an image, after hiding the information, won't degrade in quality.
- Additional information could be stored within an image.

VII. METHODOLOGY

A. AES Encryption Algorithm

AES is founded on a design principle referred to as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES doesn't |work with a Feistel Network. AES operates on a 4×4 column-major order matrix of bytes, termed their state, however some versions of Rijndael have a more substantial block size and have additional columns in the state. Most AES calculations are done in a particular finite field. We use 128bit key for an AES cipher which specifies the amount of repetitions must be 10 cycles' transformation rounds that convert the input, called the plaintext, into the last output, called the cipher text. Each round contains several processing steps, each containing four similar but different stages, including the one that is dependent upon the encryption key itself. A couple of reverse rounds are placed on transform cipher text back to the initial plaintext utilizing the same encryption.

B. Least Significant Bit Algorithm

Least Significant Bit (LSB) based steganography the simplest and most frequent form of steganography is LSB (least significant bit). Here, the components of the image are directly embedded into least significant bit plane of the cover-frame in a deterministic sequence. Modulating the smallest amount of significant bit can't be identified in human perceptible difference as the amplitude of the change is small. In this technique, the embedding capacity may be increased by utilizing several least significant bits. At once, not just the chance of creating the embedded message statistically detectable increase but additionally the image fidelity degrades. Hence a variable size LSB embedding schema is presented, by which the amount of LSBs employed for message embedding/extracting is dependent upon the area characteristics of the pixel. The benefit of LSB-based method is simple to implement and high message pay-load. Although LSB hides the message such a way that the humans don't perceive it, it is still feasible for the opponent to retrieve the message as a result of simplicity of the technique.

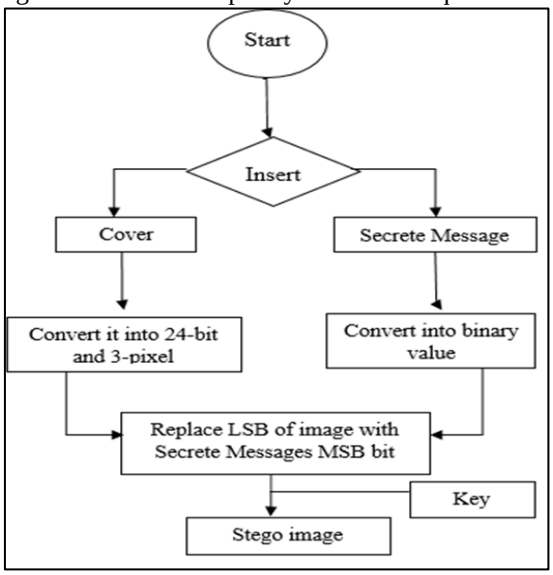

Fig. 1: LSB algorithm

5.Steganography system

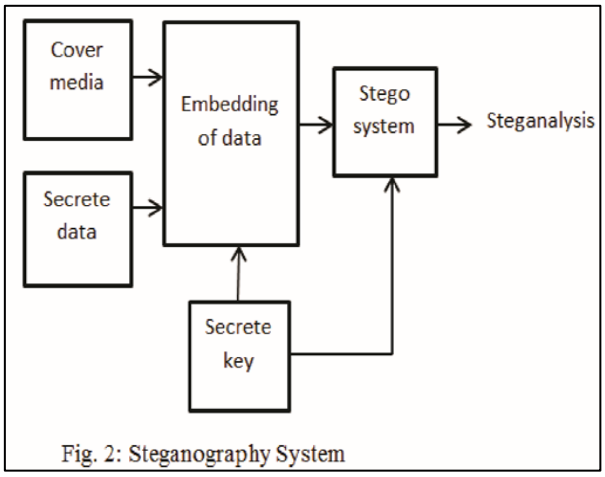

Fig. 2: Steganography System

VIII. DATA HIDING SYSTEM

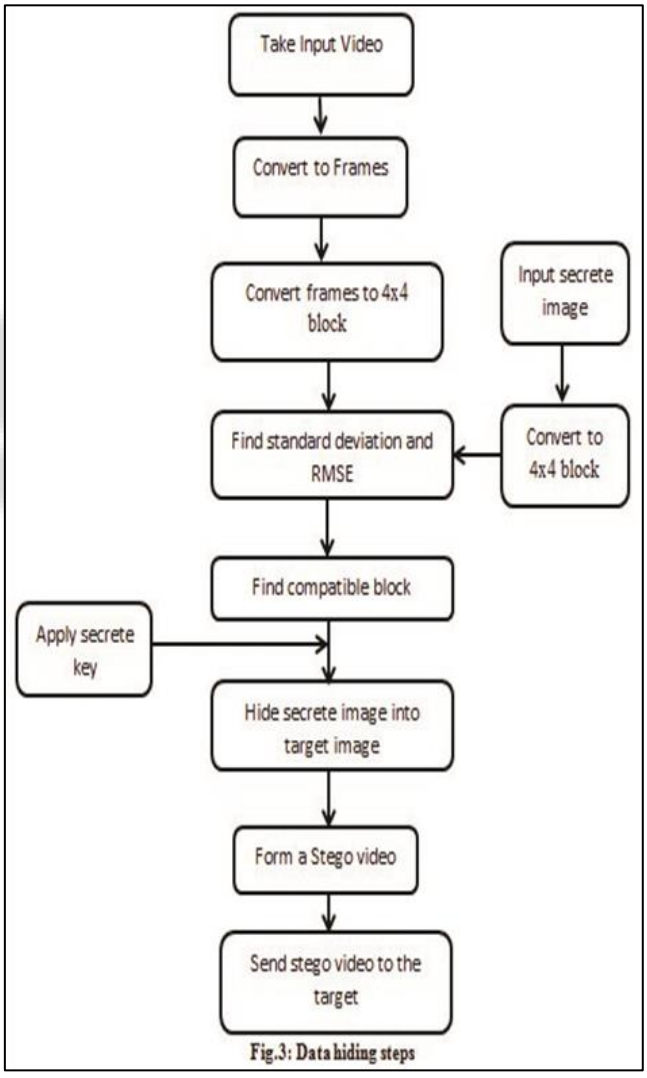

Fig.3: Data hiding steps

IX. ALGORITHMS

A. Data Embedding Algorithm

- Input: data m, image block t
- Output: stego image
- step1: F {f1, f2, f3...}
- step2: F store in 4x4 block

- step3: I_{key} store in4x4 block
- step4:mean value $\mu=\frac{1}{n}\sum_{i=1}^{n} Pi$
- $\sigma 2 = \frac{1}{n}\sum_{i=1}^{n}(P_i - \mu)^2$
- step5: Root mean squared Error
- RMSE= $\sqrt{\frac{\sum_{i=1}^{n}(P_M - P_T)^2}{n}}$
- step6:Find C_b=compatible block
- step7: store frames F= {R, G, B}
- R=red channel, G=green channel, B=blue channel
- step7: compute s
- s=m-t
- step8: If s=0
- then data is hidden and stop.
- step9: F_{RGB} get converted into S_{vdo}

B. Extraction of Data

- Input: S_{vdo}
- Output : H_{data}
- Step 1: Key1=f_i
- Step2: separate F_{RGB} into R,G,B channel
- Step3: select $B_{channel}$ of F_{RGB} for data hiding
- Step4: key2=swap position of $B_{channel}$
- Step5: Apply LSB for Extraction of data
- Step6: Apply AES for Decryption.

X. Future Scope

Secure key distribution mechanism can be implemented. Secret data can be embed randomly in a cover file to make data extraction more difficult. In Proposed method we can modified the different video format. In future work efforts can take to again improve payload capacity with minimal distortion.

XI. Conclusion

Generally, steganography is employed to transfer secret information in communication system. In this paper, a video steganography method has been developed to transfer the secret data. Text, image, audio and video can be studied as the secret data which is often hidden in the video clips. In this scheme, though, least significant bit method is employed for data hiding. LSB approach to data hiding is not secure method for data hiding therefore in this approach random frames selection algorithm and pixel swapping algorithm is incorporated to improve the security with this method. Moreover, the data itself is encrypted before embedding operation to produce this method more secure. The modification in the present method enhanced the security.

Acknowledgment

We owe a great many thanks to a great many people who helped and supported us during our project work. Our deepest thanks to the Guide of the project Prof. R. R. Rathod for guiding and correcting various documents with attention and care. He has taken pain to go through the project and make necessary correction as and when needed. We would like to thank our HOD Prof. M. R. Shimpi for providing us with a platform on which we could conduct research extensively on a topic of our choice. We express our thanks to the Principal Dr. A. S. Goje, for extending his support. We would also thank our College and our faculty members without whom this project would have been a distant reality. We also extend our heartfelt thanks to our family and well-wishers.

References

[1] H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes," in Image and Signal Processing (CISP), 2011 4th International Congress on, 2011, pp. 1784-1787.
[2] C. Chin-Chen, T. D. Kieu, and C. Yung-Chen, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," in Electronic Commerce and Security, 2008 International Symposium on, 2008, pp. 16-21.
[3] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "An Adaptive Matrix Embedding for Image Steganography," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 642-646.
[4] W. Jyun-Ji e, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," in ITS Telecommunications (ITST), 2012 12th International Conference on, 2012, pp. 365-369.
[5] C.S. Lu: Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Artech House, Inc (2003).
[6] J.J. Chae and B.S. Manjunath: Data hiding in Video. Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).
[7] Provos, N., Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine 1 (2003).
[8] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon: Secure spread spectrum watermarking for multimedia. Proceedings of IEEE Image processing (1997).
[9] J.J. Chae, D. Mukherjee and B.S. Manjunath: A Robust Data Hiding Technique using Multidimensional Lattices. Proceedings of the IEEE Forum on Research and Technology Advances in Digital Libraries, Santa Barbara, USA (1998).
[10] Y. Wang, E. Izquierdo, "High-Capacity Data Hiding in MPEG-2 Compressed Video", 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.
[11] Hideki Noda, Tomonori Furuta, Michiharu Niimi, Eiji Kawaguchi. Application of BPCS steganography to wavelet compressed video. In Proceedings of ICIP'2004. pp.2147-2150
[12] D.E. Lane "Video-in-Video Data Hiding", 2007.
[13] R. Kavitha, A. Murugan, "Lossless Steganography on AVI File Using Swapping Algorithm," Computational Intelligence and Multimedia Applications, International Conference on, vol. 4, pp. 83-88, 2007
[14] Yueyun Shang, "A New Invertible Data Hiding in Compressed Videos or Images," icnc, vol. 5, pp.576-580,

Third International Conference on Natural Computation (ICNC 2007), 2007.
[15] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb "A Secure Covert Communication Model Based on Video Steganography," in Military Communications Conference, 2008. MILCOM. IEEE on 16-19 Nov. 2008.
[16] A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, A digital watermark, Proceedings of ICIP 1994, Austin Convention Center, Austin, Texas, Vol. II, 1994, pp. 86–90.
[17] W. Bender, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3/4) (1996) 313–336.
[18] T.S. Chen, C.C. Chang, M.S. Hwang, a virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (10) (1998) 1485–1488.
[19] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083.
[20] K.L. Chung, C.H. Shen, L.C. Chang, a novel SVD- and VQ-based image hiding scheme, Pattern Recognition Lett. 22 (9) (2001) 1051–1058.
[21] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 36 (25) (2000) 2069–2070.
[22] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.
[23] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683.
[24] Uma Sahu et al, International Journal of Computer Science & Communication Networks, Vol 5(5),348-357

