Improving Security in Video Steganography using Blowfish Algorithm and MLSB Technique

Sapanpreet Kaur Mandeep Kaur

Abstract- *Video steganography is the system that deals with secure transmission of secret information behind any cover object. In the process of video steganography ,frames of a video file has been extracted and utilized for embedding of secret information. In the process of video steganography , huge amount of data can be easily transmitted over the network. Various frames can be used for hiding secret information .In the processing of video steganography ,various approaches have been proposed in recent research that are based on statistical, region based approach, LSB, 2LSB, Randompixel and 4LSB have been used mostly for videos steganography. In the proposed work , multiple least significant approach has been used for embedding of secret information and Blowfish encryption algorithm has been used for encryption of secret information and user authentication has been validated on the basis of frame number entered by the user and secret information has been embedded behind cover object frame by dividing into R ,G ,B format. After division , multiple least significant bits have been computed and utilized for embedding of finalized secret data. Various parameters PSNR , MSE has been measured for performance evaluation of proposed work .On the basis of these parameters , one can say that proposed approach provides much better results.*

Keywords: DCT, MLSB, security, steganography.

1. INTRODUCTION

Steganography:

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in cryptography it's always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender.

A. **Cryptography:** is the practice and study of techniques for secure communication in the presence of third parties. The modern field of cryptography can be divided in to two ways: Symmetric key cryptography and public key cryptography. The symmetric key cryptography provides encryption of data at the sender and the receiver side where both share the same key. The symmetric key cryptography is implemented via block ciphers or stream ciphers. This form of cryptography has a disadvantage that it involves the key management process for the secure networking. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret .To solve the said issue, the public key cryptography came in to existence. In public key cryptography, the encryption is done through public key(which is available to all) and the secret key often referred to as private key is used to perform the decryption process. The pairing of public and private key ensures secure communication. This technology can be used to implement digital signatures scheme.

B. Steganography: is the art or practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal[4]. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.[5][6]

2. REVIEW OF LITERATURE

V. Saravanan [1] did analysis on Security Issues in Computer Networks and Stegnography. The proposed work reduces the detectable distortion in a joint photographic experts group (JPEG) file during data hiding process, by introducing new region selection rule. The new region selection rule considers three factors, i.e., the horizontal difference (HD), vertical difference (VD) and region size (RS). The JPEG image will be split into number of blocks and each pixel in it will be examined to calculate the variations. Depends upon the variation, the amount of secret information will be hide in an image. This proposed method of information hiding will help to solve the security issues in computer networks. The experimental result shows that the proposed system hides approximately 45% of secret information in addition, comparing existing methods without increasing detectable distortion.

Moon, S.K et al [3] utilized least significant bit (4LSB) substitution strategy. The 4LSB strategy is executed for shade bitmap pictures (24 bit and 8 bit i.e. 256 shade palette pictures) and wave documents as the transporter media. "The objective of steganography is to shroud messages inside different innocuous messages in a manner that does not permit any adversary to try and identify that there is a second mystery message present." By utilizing this proposed calculation, we can shroud our record of any configuration in a picture and sound document. We can then send the picture through email connection or post it on the site and anybody with learning that it contains mystery data, and who is in ownership of the encryption watchword, will have the capacity to open the document, separate the mystery data and unscramble it.

Mazen Abu Zaher [16] worked on Information Security. Their work introduces modifications to existing steganography algorithm known as LSB "Least Significant Bit". The main idea of our work is to increase amount of data that can be hiding using LSB. In addition our algorithm encrypt data before hide it, which provide another level of protection over traditional LSB technique.

Mstafa, R.J. et al [19] worked on a highly secure video steganography using Hamming code (7, 4) because of the high velocity of web and advances in innovation, individuals are getting to be more agonized over data being hacked by assailants. As of late, numerous calculations of steganography and information stowing away have been proposed. Steganography is a methodology of inserting the mystery data inside the host medium (content, sound, picture and feature). Simultaneously, large portions of the effective steganographic investigation programming projects have been given to unapproved clients to recover the significant mystery data that was installed in the bearer documents. Some steganography calculations can be effectively caught by steganalytical identifiers due to the absence of security and implanting proficiency. In this paper, we propose a safe feature steganography calculation taking into account the standard of straight square code. Nine uncompressed feature successions are utilized as spread information and a twofold picture logo as a mystery message. The pixels' positions of both spread features and a mystery message are haphazardly reordered by utilizing a private key to enhance the framework's security. At that point the mystery message is encoded by applying Hamming code (7, 4) preceding the inserting methodology to make the message significantly more secure. The consequence of the encoded message will be added to arbitrary created values by utilizing XOR capacity. After these steps that make the message secure enough, it will be prepared to be implanted into the spread feature outlines. Also, the inserting range in each one edge is arbitrarily chosen and it will be not the same as different casings to enhance the steganography plan's vigor. Moreover, the calculation has high installing proficiency as showed by the trial results that we have acquired. As to framework's quality, the Pick Signal to Noise Ratio (PSNR) of stego features are over 51 dB, which is near to the first feature quality. The installing payload is additionally worthy, where in every feature outline we can install 16 Kbits and it can go up to 90 Kbits without recognizable corrupting of the stego feature's quality.

Ramaiya, M.K et al[20] did Security improvisation in image steganography using DES" The staggering advancement of Internet innovations & its applications oblige abnormal state the security of information over the correspondence channel. Picture steganography is a computerized method for hiding data into a spread picture. Least Significant-Bit (LSB) based methodology is most mainstream steganographic method in spatial space because of its effortlessness and concealing limit. All of existing routines for steganography concentrate on the inserting procedure with less thought to the preprocessing, for example, encryption of discharge picture. The traditional calculation does not give the preprocessing needed in picture based steganography for better security, as they don't offer adaptability, power and abnormal state of security. The proposed work exhibits an one of a kind procedure for Image steganography in light of the Data Encryption Standard (DES) utilizing the quality of S- Box mapping & Secrete key. The preprocessing of emit picture is conveyed by implanting capacity of the steganography calculation utilizing two exceptional S-boxes. The preprocessing give abnormal state of security as extraction is impractical without the learning of mapping standards and discharge key of the capacity. Also the proposed plan is equipped for scrambling information as well as changes the force of the pixels which adds to the wellbeing of the encryption [16].

Balaji, R. [22] It is extremely fundamental to transmit imperative information like saving money and military data in a safe manner. Video Steganography is the methodology of concealing some mystery data inside a feature. The expansion of this data to the feature is not conspicuous by the human eye as the change of a pixel shading is unimportant. This paper means to give a productive and a safe strategy for feature Steganography. The proposed system makes a list for the mystery data and the record is put in a casing of the video itself. With the assistance of this record, the casings containing the mystery data are placed. Consequently, amid the extraction process, as opposed to examining the whole feature, the casings containing the mystery information are investigated with the assistance of list at the less than desirable end. At the point when steganographed by this strategy, the likelihood of discovering the shrouded data by an aggressor is lesser when contrasted with the typical technique for concealing data outline by-edge in a successive way. It additionally diminishes the computational time taken for the extraction process.

Malik et al. [23] proposed two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. But in some cases if the eavesdropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form. For cryptography Blowfish algorithm is used which is much better than AES and DES. In order to break blowfish algorithm he has to spend a lot of time and effort for trying several attacks and getting the original message. Although both of these techniques are easy to implement but there combination will provide much efficient and reliable security.

Pratap Chandra Mandal [24] Evaluated of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. Author presented the performance evaluation of selected symmetric algorithms. It can be concludeds that Blowfish has better performance than other algorithms. Secondly, AES has advantage over the other 3DES and DES in terms of throughput & decryption time except Blowfish. Third point is that 3DES has the least performance among all the algorithms mentioned here.

3. METHODOLOGY

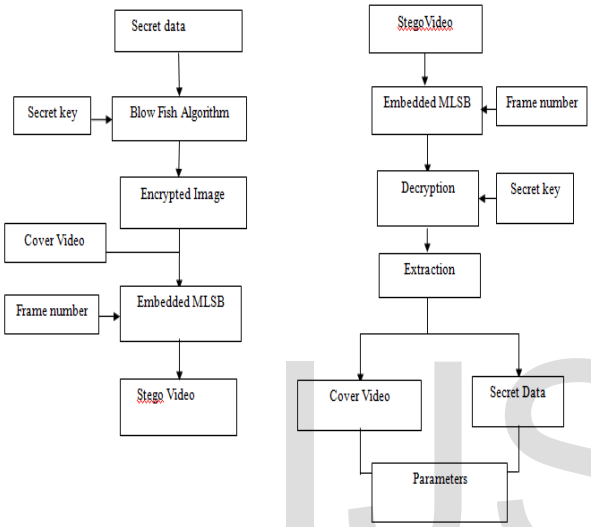

Fig 3.1: Flow diagram for proposed work

Phase 1: Load the cover image and select the secret image. Selected cover video and secret image should be in RGB format.

Phase 2: Blowfish Encryption Algorithm is applied on the secret image for enhancing the security. The user manually enters the secret key for encryption.

Phase 3: The encrypted secret image is embedded in the cover video using **Multiple least significant bit.** For authentication, the user manually specifies the frame number. All the pixel values of the specified frame number are evaluated on the basis of intensity values of R, G and B components and the appropriate pixels are selected for embedding the secret data. Hence a stego video is generated for secure transmission of data.

Phase 4: On the receiving end, the user specifies the frame nusmber to extract the frame behind which the secret image was embedded and then applies the secret key to decrypt the encypted sent image and finally parameter analysis is performed .

4. RESULTS

4.1 PSNR: PSNR stands for peak signal to noise ratio. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. PSNR is usually expressed in terms of the logarithmic decimal scale. PSNR is used to measure the quality of stego-image or stego-video. The signal or input in this case is the original data, and the noise is the error introduced by compression[16].

Table 4.1: Parameters Comparison on the basis of PSNR

Cover Object	MLSB	4LSB
Video 1	23.68	16.69
Video 2	35.69	25.60
Video 3	59.98	48.96
Video 4	33.78	26.58
Video 5	53.48	29.69

Table 4.1 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter PSNR has been evaluated for different images and values has been represented in tabular form for proposed and existing technique.

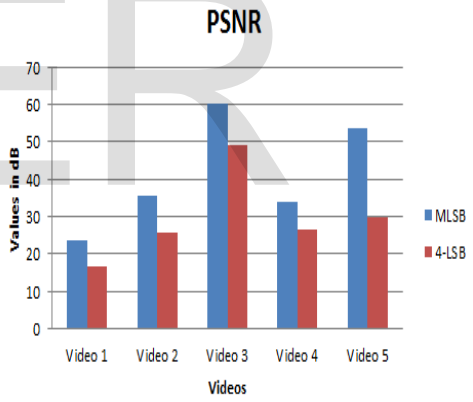

Fig 4.1 Comparison graph of proposed work with existing using PSNR

Figure 4.1 represents graphical representation of performance evaluation parameter correlation with existing approach. As graph represents proposed wok provide better PSNR than existing approach.

4.2 MSE: Mean square error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. It is basically a difference between the cover image/video and stego image/video. If the value of MSE is low, then the quality of the stego image/video is better[13].

Table 4.2 Parameters Comparison on the basis of MSE

Cover Object	MLSB	4LSB
Video 1	0.24	1.56
Video 2	0.36	0.98
Video 3	0.25	2.6
Video 4	0.69	1.26
Video 5	0.33	0.96

Table 4.2 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter MSE has been evaluated for different images and values has been represented in tabular form for proposed and existing technique

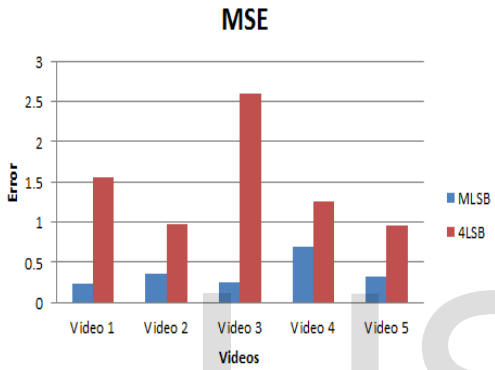

Fig 4.2 Comparison graph of proposed work with existing using MSE

Figure 4.2 represents graphical representation of performance evaluation parameter MSE with existing approach. As graph represents proposed wok provide less mean square error than existing approach.

5. CONCLUSION & FUTURE SCOPE

5.1 CONCLUSION

The meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. In the proposed work, video steganography has been used for secure transmission of secret information. In the process of video steganography, secret information has been embedded behind the cover video pixels.

In the proposed work, cover video has been selected for embedding of secret information behind pixels of the video. Cover video has been divided into different color regions in order to extract red, green and blue region pixels. After division into these color images parts have been utilized in single manner so that data can be embedded behind the pixels o f the RGB colors. Secret image has been encrypted by using Blowfish Encryption Algorithm for secure aspects. Blowfish Encryption Algorithm is a symmetric-key block cipher and is one of the most secure encryption algorithms. After encryption of secret information, data has been embedded behind the cover object pixels.

In the process of embedding multiple least significant bits have been extracted from all color segments of cover object. These different color pixel values have been divided into different binary format, so that multiple least significant bits can be computed. All the color region has been used and according to intensity levels, data has been embedded behind the cover pixels. To develop more secure steganography, user authentication has been validated in the proposed work that provides the user to manually enter the frame number whose pixels can be manipulated. The frame number has been transmitted to the authenticated user via message or mail. If a valid user provides the correct frame number only then he/she is able to extract data from cover object.

The proposed work has been compared with various previous approaches on the basis of performance evaluation parameters. As illustrated from results, proposed work provides much secure steganography than previous LSB, 2LSB, 4LSB data embedding approaches. So by analyzing parameters one can conclude that proposed work provides much better results than previous approaches utilized for video steganography.

5.2 FUTURE WORK

In the future reference steganography can be done by using proposed approach in real world scenario. In the future new approaches can be used for evaluation of region in the video that can be used for hiding of secret information. For extraction of region classification can be done on the video file that extract important and less important region for video quality.

REFRENCES

[1] Saravanan,V, Neeraja, A. "Security issues in computer networks and stegnography" *IEEE 7th International Conference onIntelligent Systems and Control*, pp. 363-366, 2013.

[2] XikaiXu, Wei Wang, Tieniu Tan "Video steganalysis based on the constraints of motion vectors" *20th IEEE International Conference onImage Processing*, pp. 4422-4426, 2013.

[3] Moon, S.K, Kawitkar, R.S. "Data Security Using Data Hiding" *IEEE International Conference on Computational Intelligence and Multimedia Applications*, vol. 4, pp. 247-251, 2007.

[4] Gupta, Rupesh, TanuPreet "New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters" *IEEE International Conference on Contemporary Computing and Informatics*, pp. 475-479, 2014.

[5] Marwaha, P. "Visual cryptographic steganography in images", *IEEE Second International conference on*

Computing, Communication and Networking Technologies, pp. 34-39, 2010.

[6] Bailey, K. "An evaluation of image based steganography methods", *Journal of Multimedia Tools and Applications*, Vol. 30, No. 1, pp. 55-88, IEEE, 2006.

[7] Md. Rashedul Islam, AyashaSiddiqa, Md. PalashUddin "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" *IEEE3rd International Conference on Informatics, Electronics & Vision*, pp. 1-6, 2014.

[8] Mehdi Hussain, Mureed Hussain "Pixel Intensity Based High Capacity Data Embedding Method" *IEEE International Conference on Information and Emerging Technologies*, pp. 1-5, 2010.

[9] Asad, M, Gilani, J. , Khalid, A. "An enhanced least significant bit modification technique for audio steganography" *IEEE International Conference on Computer Networks and Information Technology,* pp. 143-147, 2011.

[10] Artz, D "Digital steganography: hiding data within data" *IEEE Internet Computing*, vol 5, pp. 75-80, 2001.

[11] Yang Ren-er, Tao Shun, Ding Shilei "Image Steganography Combined with DES Encryption Pre-processing" *IEEE Sixth International Conference on Measuring Technology and Mechatronics Automation*, pp. 323-326, 2014.

[12] Guo, J.-M, Jen-Ho Chen "Quality Compressed Steganography Using Hidden Referenced Halftoning" *Ninth IEEE International Symposium on Multimedia*, pp. 273-281, 2007.

[13] Mathkour, H, Al-Sadoon, B. , Touir, A. "A New Image Steganography Technique" *IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing,* pp.1-4, 2008.

[14] Bandyopadhyay, S.K. ,Tai-hoon Kim , Parui, S. "Network Based Public Key Method for Steganography" *IEEE International Conference on Ubiquitous Computing and Multimedia Applications*, pp. 53-56, 2011.

[15] Fard, A.M, Akbarzadeh-T, M.-R. , Varasteh-A, F. "A New Genetic Algorithm Approach for Secure JPEG Steganography" *IEEE International Conference on Engineering of Intelligent Systems*, pp. 1-6, 2006.

[16] Mazen, A. Z. "Modified Least Significant Bit (MLSB)" *IEEE Conference on MLSB*, pp 60-67, 2011.

[17] Changder, S, Debnath, N.C. , Ghosh, D. "A Greedy Approach to Text Steganography Using Properties of Sentences" *IEEE Eighth International Conference on Information Technology: New Generations*, pp. 30-35, 2011.

[18] Banerjee, S, Chakraborty, M.S. , Das, S. "A variable higher bit approach to audio steganography" *IEEE International Conference on Recent Trends in Information Technology*, pp. 46-49, 2013.

[19] Mstafa, R.J, Elleithy, K.M. "A highly secure video steganography using Hamming code (7, 4)" *IEEE Long Island Systems, Applications and Technology Conference,* pp. 1-6, 2014.

[20] Ramaiya, M.K, Hemrajani, N. ,Saxena, A.K. "Security improvisation in image steganography using DES" *IEEE 3rd International Advance Computing Conference,* pp. 1094-1099, 2013.

[21] Uddin, M.P, Fserdousi, S.J. , IbnAfjal, M. "Developing an efficient solution to information hiding through text steganography along with cryptography" *IEEE 9th International Forum on Strategic Technology*, pp. 14-17, 2014.

[22] Balaji, R. "Secure data transmission using video Steganography" *IEEE International Conference on Electro/Information Technology (EIT)*, pp 1–5, 2011.

[23] Malik, S. and Singh, A. "Securing Data by Using Cryptography with Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol 3, Issue 5, 2013.

[24] Pratap Chandra Mandal "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" *Journal of Global Research in Computer Science,* Vol 3, No. 8, 2012.