IJCTA, 9(26) 2016, pp. 57-65

Secured Video Data Hiding Using Cryptography Algorithms

K. Maheswari[1] and R. Thamarai Selvi[2]

ABSTRACT

A huge variety of stenographic techniques exists for hiding data in an appropriate carrier such as text, image, audio, and video sent to a receiver secretly. The steganography provide as one of the best method to share the data secretly and securely. The current work signifies cryptography of audio and video which is a arrangement of image steganography, audio and video cryptography by making use of Technique as a tool for clients. The main aim is to hide secure data behind image and audio of video file. Video is a operation of many still frames of images and audio, video thus for hiding secret data any frames can be selected for audio and video. Appropriate algorithm such as combine Digital Encryption Standard and Triple Digital Encryption Standard for security and authentication image processing is used hence data security can be increased.

Keywords: Steganography, Cryptography, Audio-Video Steganography, Digital Watermarking, StegoVideo

I. INTRODUCTION

Data hiding is the development of embedding information into a host medium. In normally visual and aural media are preferred due to their wide company and the tolerance of human perceptual systems involved. Data hiding in video sequences is performed in two main ways: Bit stream-level and Data-level. The new compression standards are exploited. Typically, encode have various options during programming and this freedom of selection is well for manipulation with the aim of data hiding. These methods very much rely on the structure of the bit stream hence, they are quite easily broken, in the sense that in many cases they cannot carry on any format exchange or transcoding even exclusive of any significant loss of perceptual value. Result, this type of data hiding method is generally proposed for fragile application, such as authentication. On the additional data-level methods are more robust to attacks.

1.1 Steganography

It is the process of secretly embedding information inside a data source without changing its perceptual superiority. It's comes from the Greek word stegano which accurately means "covered" and graphic which means "writing", i.e. covered writing. The majority common use of steganography is to hidden a file within another file.

A. Text steganography

It is hiding information in text the most important method of steganography. The method was to hide a secret message in each nth letter of each word of a text message.

B. Audio steganography

When developing a technique for audio steganography one of the first considerations is the likely environment, the sound signal will journey in environments between encoding and decoding.

[1] Research Scholar, Computer Science, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India

[2] Head & Assistant Professor, Department of Computer Applications, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India

C. Image/Video steganography

Images are often use as the accepted cover objects in steganography. A message is embedded in a digital image through various embedding algorithms and a secret key.

D. Data Hiding Techniques in IPv4 Header

To strongly transmit the data over the network the Vasudevan et al. it used the analogy of the jigsaw puzzle.

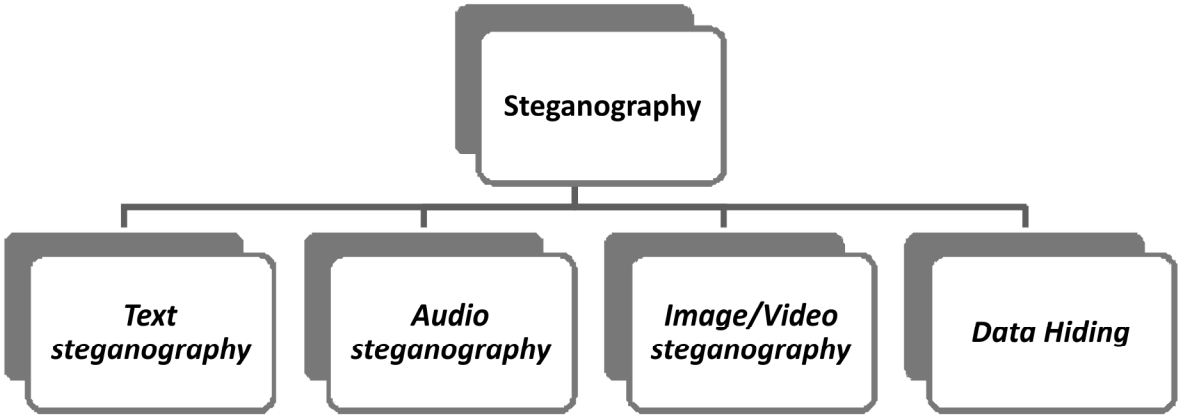

Figure 1: Steganography Type

1.2 Cryptography

It is the practice and study of techniques for secure message in the presence of third parties. More usually, it is about construct and analyzing protocols that overcome the influence of adversaries and which are connected to a variety of aspects in information safety such as data confidentiality, data integrity, authentication, and non-repudiation. Present cryptography intersect the disciplines of mathematics, computer science, and electrical engineering.

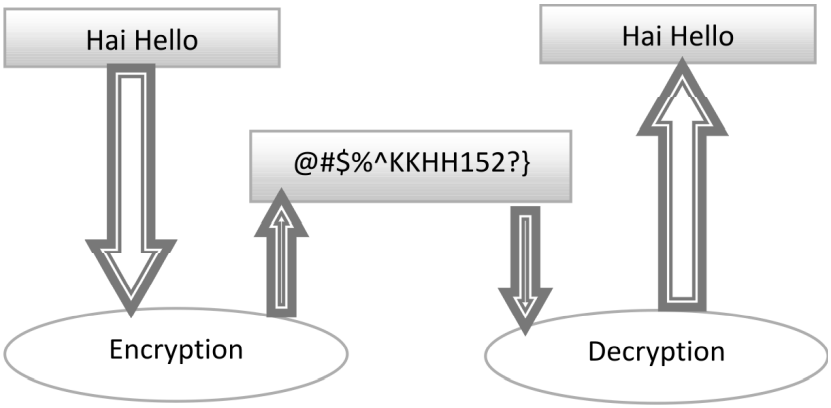

Figure 2: Cryptography Diagram

2. RELATED WORK

In [3] a steganographic scheme was proposed, it uses being vision sensitivity to hide secret bits. To make this, the top secret data firstly are converted into a series of symbols to be embedded in a notation system with multiple bases.

In [4] this case, the particular bases used is determined by the degree of local variation of the pixel magnitudes in the host image. A updating to the least significant bit matching (LSBM) steganography was introduced.

This [5] modification provides the most wanted choice of a binary function of two cover pixels rather than to be random as in LSBM. To enlarge the level of protection, a combined data encoding and hiding process was proposed.

This [6] process was used to overcome the difficulty of image color change after the embedding process. The LSB steganography technique was developed. it based on embedding the top secret message into the sharper edge region of the image to ensure its conflict against image stego analysis based on statistical analysis.

A novel image steganography was projected in [7], it is based on integer wavelet transform [IWT], it is used to embed more than a few secret images and keys in color cover image. A quantization based steganography method presented.

In [11] and [12] two protected message systems were proposed to be used for voice over IP (VOIP) application. LSB based steganography was employed to hide the data over an audio cover indicator. An extended version of SHA-1 (Secure Hash Algorithm) was introduced in; this system can be used to encrypt two dimensional records such as image. It is developed to enlarge the resistance of image based steganography against the attackers and hackers.

A chaotic signal was working in [13] for picture steganography, which presents a scattering arrangement for the embedded information through the cover imaged. A high capacity and security steganography using discrete wavelet transform (HCSSD) was developed in the wavelet coefficients for the cover image and the payload image were combined to obtain a single image. All authors in have proposed a two level data security comprise of text cryptography and images steganography. The very secret text is encrypted using Blowfish algorithm followed by embedding it into an images using LSB encoding. The carrier figure can be then transmit over the network.

In [14], authors have suggested an algorithm in which the records is first subjected to encrypt using Data Encryption Standard (DES). The encrypted message is then passed to embedding phase. In embed phase the encrypted message will embedded into the cover intermediate which is either image is extracted at the receiver side.

3. PROPOSED WORK

A new algorithm is implementing for better information security and transfer of data from source to destination. The good approach to video cryptography with video file should aim at concealing the topmost

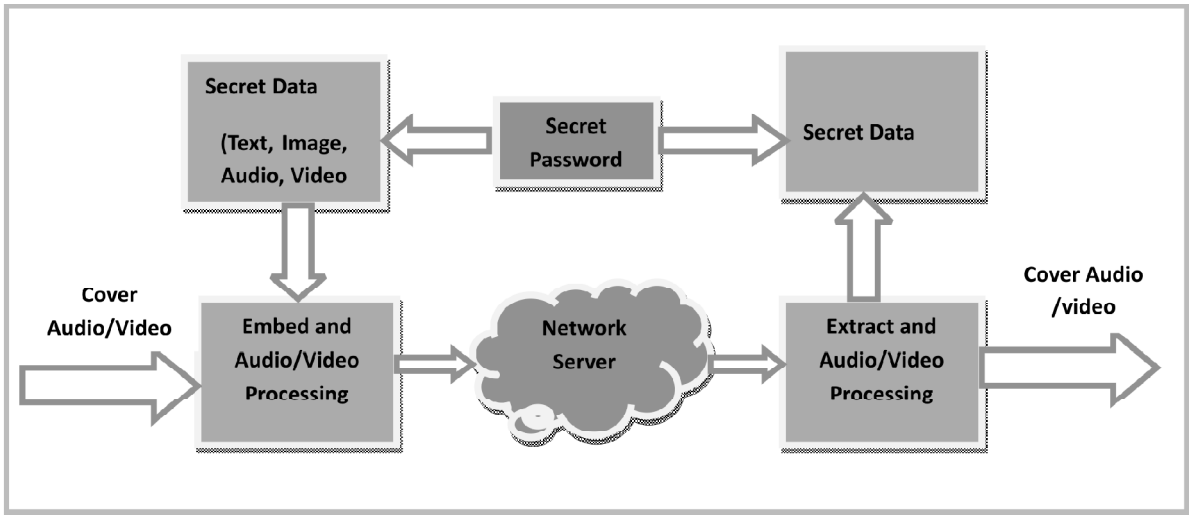

Figure 3: System Architecture

amount of data possible in a cover video while maintain imperceptibility, that is an up to standard level of visual quality for the video. Data hiding in video sequences is perform in two main ways: bit stream-level and data-level. In this concept propose a new block-based selective embedding type data hiding structure that encapsulates algorithm. By means of simple rules applied to the frame marker, we introduce certain height of robustness against frame drop, repeat and insert attacks.

- In present system, the client sends data from one system to another system in Local Area Network.
- Because of the protection issues not only certified persons but also unauthorized persons can view the data.

The use of cryptography application is to hide the different type of data within a cover file. The resulting stego applications do contain the hidden information, although it is virtually identical to the cover file.

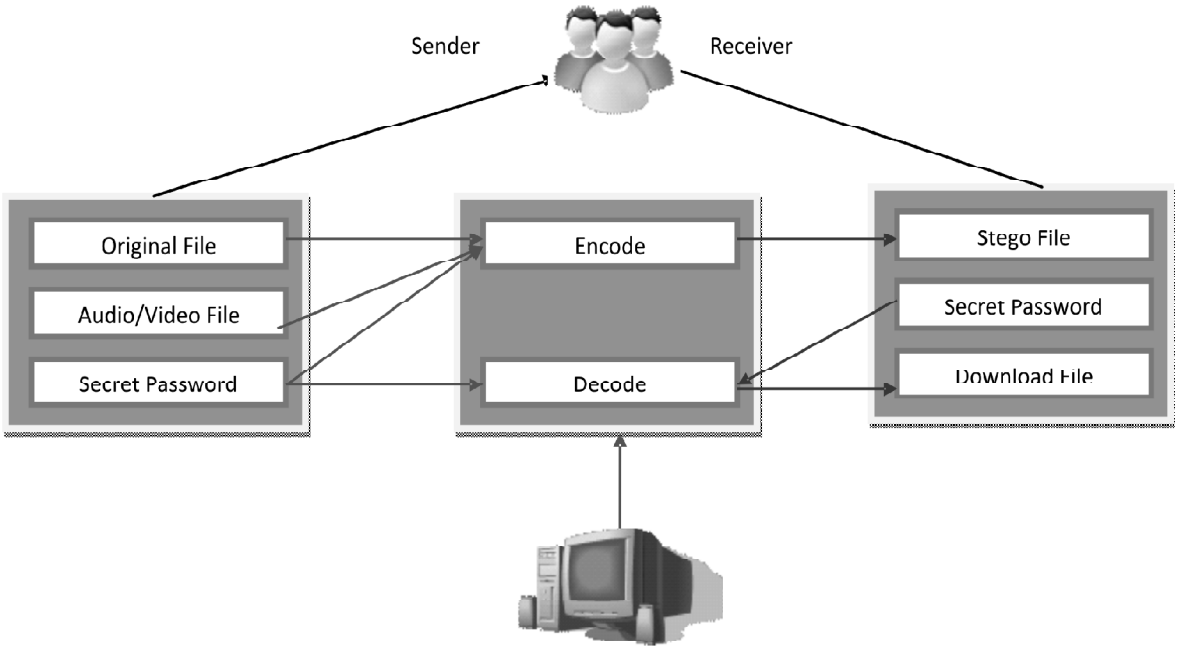

Figure 4: Process flow of Audio/Video Cryptography

In the process flow audio/video diagram describes user provide his input video file , text data and security key for hiding data into Video. The procedure of system is to collect necessary input from user and Encode the data into Video and Generate Stego Video Similar to Input Video. Receiver wants to decode it then user needs to provide stego video file and security key which is already used for programming process.

3.1. Proposed Algorithm Step For Data Security

Hiding method for hidden information (Embedding Process)

The embedding procedure takes a cover video and a secret message as the inputs.

Step 1: First take an original file

Step 2: Load a secret file which embeds into the cover video and designation source.

Step 3: Add a password in number format for more security.

Step 4: Then apply the technique. The techniques video file bit of the replaced by the binary data. Then get a stego video file.

Step 5: At last, have a video file. This video is ready for the transmission through the receiver .

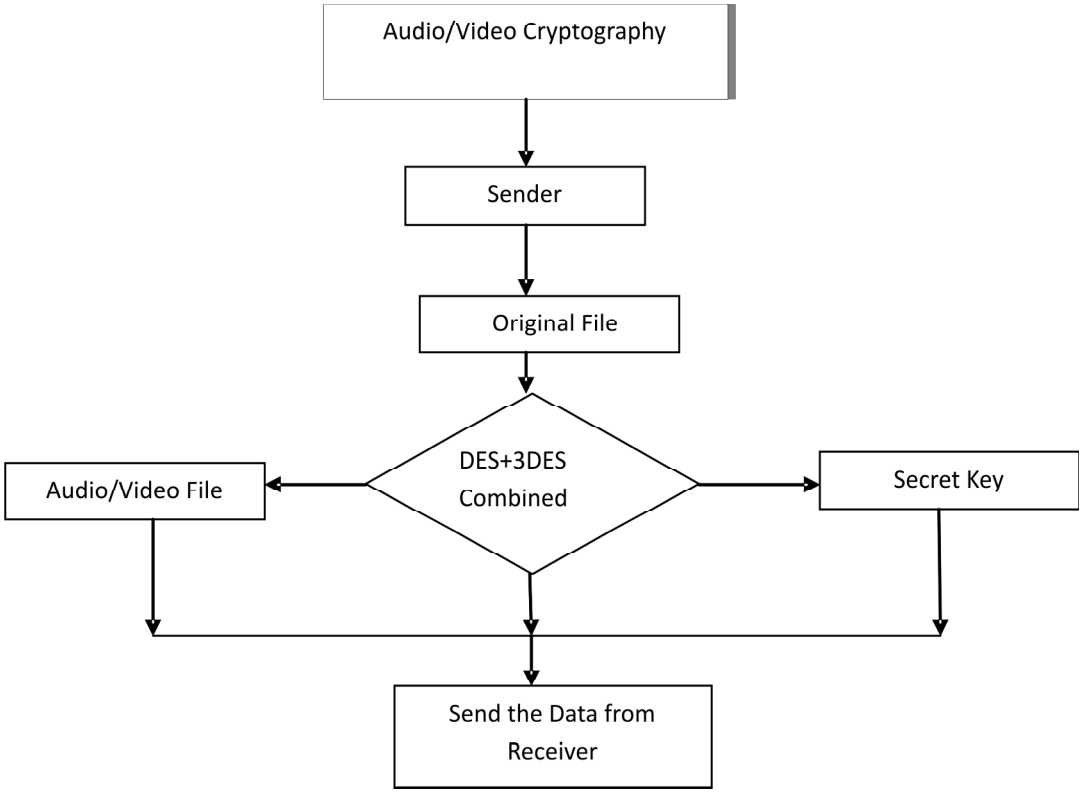

Figure 5: Data Flow Diagram (Embedding Process)

Un Hiding method of hidden information

It basically follows the reverse process of the hiding algorithm to obtain the secret message or file. Steps to get well the hidden information:

Step1: Load the stegno video.

Step2: Enter the password to get the secret message.

Step3: Implement the technique to get the stegno video

Step5: Get the secret message and original video.

Step 6: Finally analyze the result on the basis of combined DES+3DES and histogram.

3.2. Proposed Algorithms Combined DES and 3DES

ALG= Digital Encryption Standard +Triple Digital Encryption Standard

- ✓ ALG is used to do Encryption and decryption of data in 64-bit block of cipher text
- ✓ ALG has 16 rounds, means the algorithm is repeated 10 times to get the cipher text
- ✓ It has been observe that the number of rounds is proportionally exponential to the total of time required to find a key.
- ✓ If the number of rounds increase, the security of the algorithm will increase exponentially
- ✓ This project “ALG” is based on client server technology
- ✓ The sender will send the encrypted file using internet link On the other side the receiver will received the file and decrypts the file by using the same private key used by the sender.

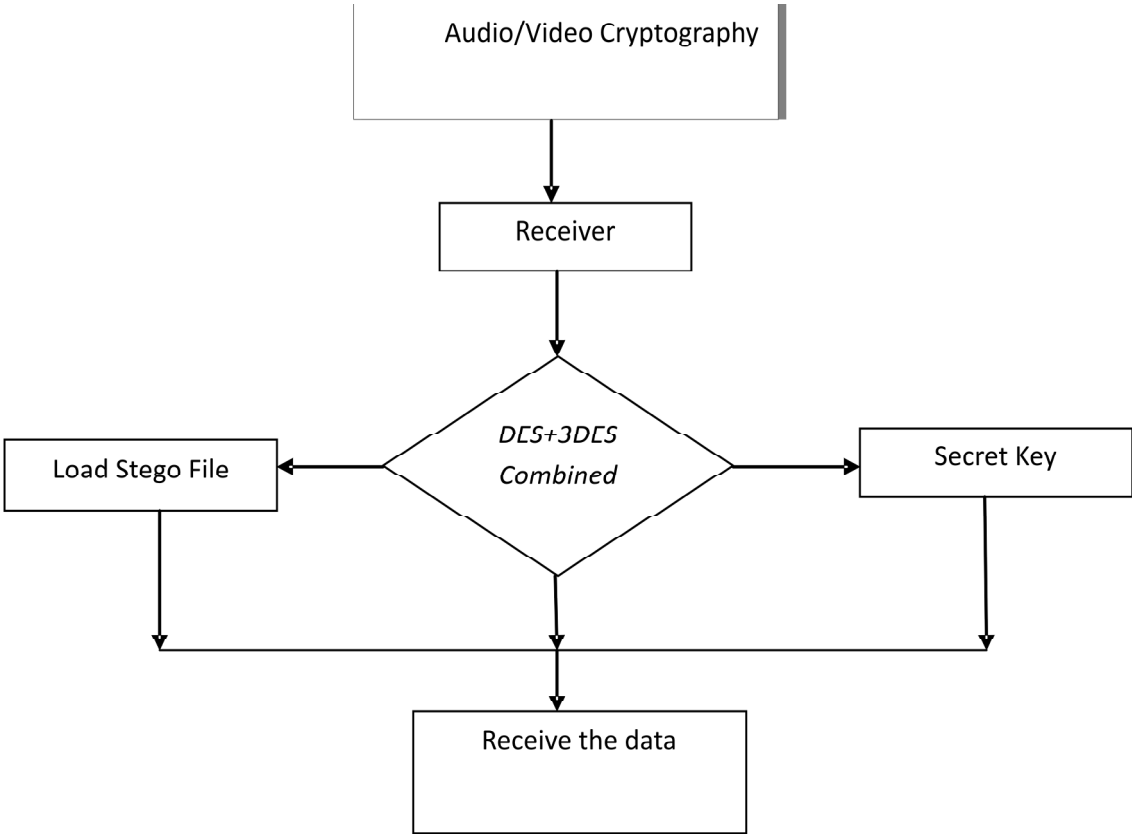

Figure 6: Data flow diagram Unhiding Process

IV. COMPARATIVE ANALYSIS

Table 1
Comparisons of Video Encryption Scheme

Algorithm	*Capacity*	*Speed*	*Secure*	*Cover image*	*Secret image*	*Encryption*
Secured data transmission (SDT)	Better	Slow	Less secure	AVI	Image	75%
Hybrid Encryption and Steganography (HES)	High	Fast	Secure	AVI	Text	75%
LSB Polynomial Equation Algorithm (LSBPOLY)	Low	Slow	Less secure	AVI	Text	70%
Hashed-based LSB (HLSB	Good	Very Fast	Less secure	AVI	Text	73%
Multiple LSB (MLSB)	Good	Fast	Less secure	AVI	Text	65%
LSB Matching Revised Algorithm (LSBMR)	High	Very Fast	Secure	FLV	Text	75%
Novel Video Steganography (NVS)	High	Very Fast	High secure	AVI, MPEG, MOV, FLV	Text, image, audio, and video	83%
Present Work	Very High	Super Fast	Very High Secure	All Files	All Files	90%

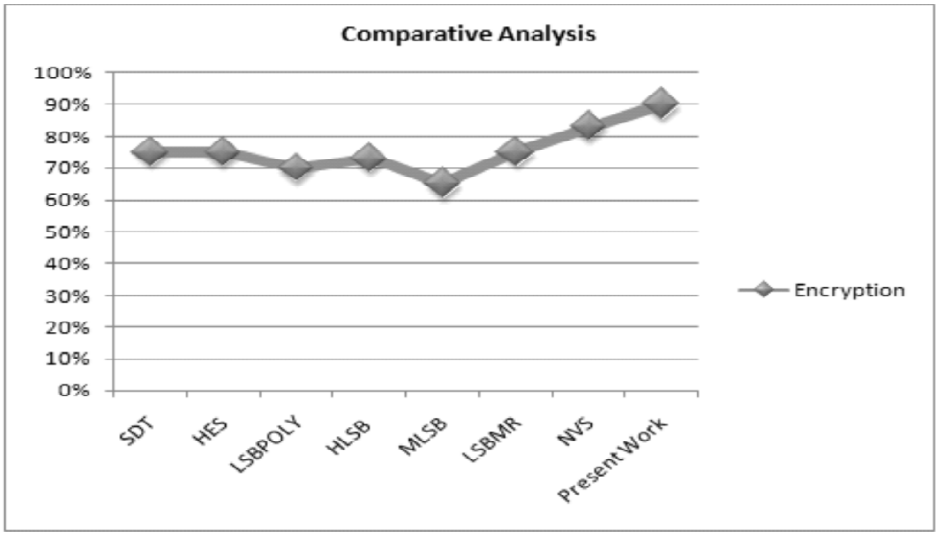

Chart 1: Comparisons of Video Encryption Scheme

4. EXPERIMENT AND RESULTS

The proposed method has been implemented using JAVA Technology. It Should Performance of theoretical design is turned out into a effective system. Thus it can be careful to be the most critical stage in achieving a successful new system and in giving the client, self-assurance that the new system will work and be effective. The implementation stage involves careful planning, investigation of the previous system and it's constraints on implementation, designing of method to achieve changeover and evaluation of methods. For more security provides by combined algorithm DES and Triple-DES is at present one of the favorite public key encryption methods.

Time Report

Table 1 shows the time analysis of the above algorithm, time analysis is performed on the **Table 1** values.

Table 1
Time Analysis Table

S. No.	*File Size*	*Encryption Time*	*Decryption Time*	*Encryption /Byte*	*Decryption/Byte*
1	250MB	0.25	0.24	0.0000125	0.0000135
2	500MB	0.23	0.22	0.0000128	0.0000126

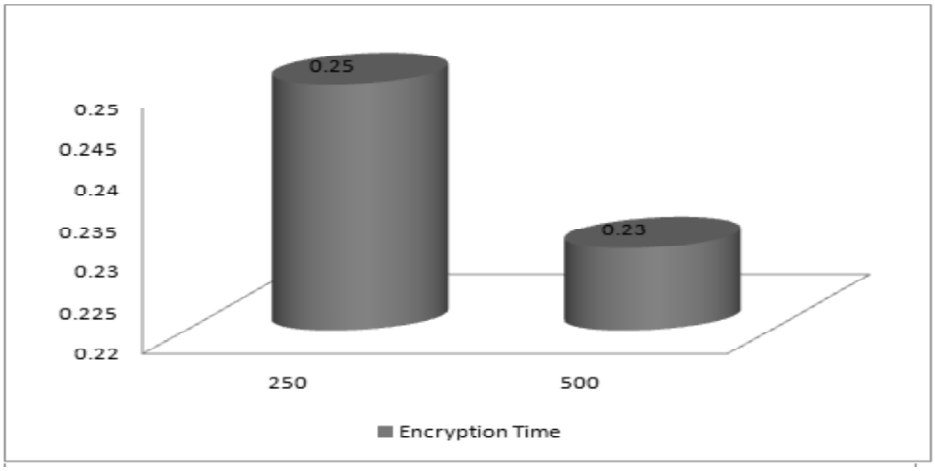

Chart 1: Encrypted Time Analysis Graph

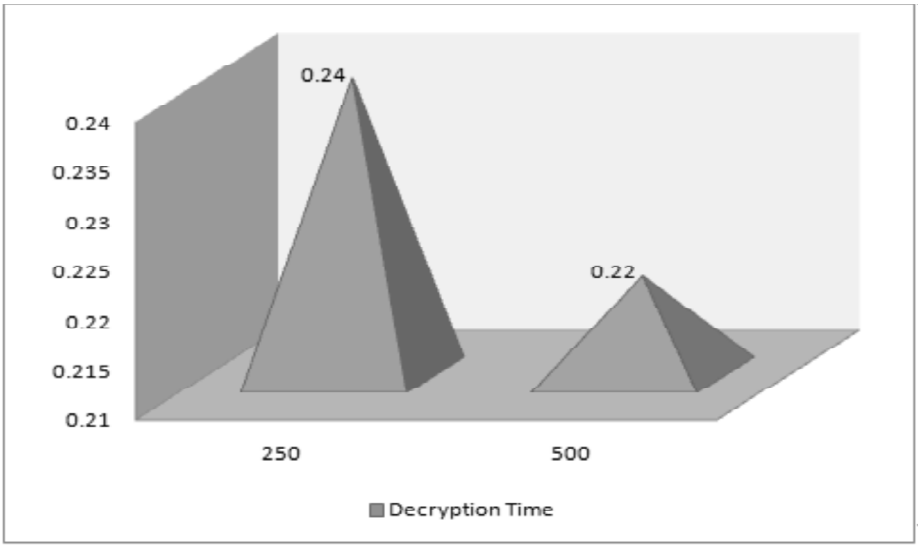

Chart 2 : Decrypted Time Analysis Graph

CONCLUSION

This proposed work new video data hiding framework that makes use of erasure correction capability of present codes and superiority of more flexibility. In the system of fast information interchange using sender and receiver, video cryptography has become essential tool for information protection. This study gave an overview of different video cryptography techniques its main type and classification proposed in the literature during last few years. The algorithm is also video to frame manipulation attacks via frame synchronization markers. The results indicate that the framework can be effectively utilized in video data hiding applications.

REFERENCES

[1] Abdul Qadir, Ishtiaq Ahmad., "digital text watermarking: protected content delivery and data hiding in documents ", *IEEE*, 2012.

[2] Jayeeta Majumder. Sweta Mangal., "An Overviews of Image Steganography using LSB Techniques", *International Journal of Computer Applications*, 2012.

[3] R. Ravi Kumar V. Kesava Kumar., "Selective Embedding and Forbidden Zone Data Hiding for Strong Video Data Thrashing", *International Journal of Engineering Trends and Technology*, **4(1)**, 2013.

[4] Mr. Sudheer Adepu. Mr.P. Ashok. Dr.C.V.Guru Rao., "A Security Method for Video information hiding", *International Journal of Computer Trends and Technology*, 2013.

[5] Resoju Omprakash. D. Jyothi., "Block Based Adaptive Video records thrashing Technique", *International Journal of Medical Sciences and Technology*, 2012.

[6] Mr. Mritha Ramalingam., "Stego Machine Video Steganography using Modified LSB Algorithm", *World Academy of Science, Engineering and Technology*, 2011.

[7] W. Bender. D. Gruhl. N.Morimoto,A. Lu., "Technique for data hiding ", *IBM SYSTEMSJOURNAL*, **35(3)**, 2011.

[8] Tong L. Zheng-ding., "DWT-based color Images Steganography Scheme", *IEEE International Conference on Signal Processing*, 2002.

[9] Mandal J.K. Sengupta .M., "Authentication Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC)", *Proceedings of International convention on Electronic System Design, IEEE meeting Publications*, 2010.

[10] Septimiu F. M. Mircea Vladutiu. Lucian P., "Secret data communiqué system using Steganography, AES and RSA", *IEEE 17th International Symposium for Design and Technology in Electronic Packaging*, 2011.

[11] H. Tian, K. Zhou, Y. Huang. D. Feng, J. Liu., "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", *IEEE The 9th International discussion for Young Computer Scientists*, 2008.

[12] Y. Huang. B. Xiao. H. Xiao., "Implementations of Covert Communication Based on Steganography", *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2008.

[13] Z. Wei. K. N. Ngan., "Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Video in DCT Domain", *IEEE transaction on Circuits and Systems for Video Technology,* 337—346, 2009.

[14] M. Maes, T. Kalker. J. Haitsma. G. Depovere., "Exploiting Shift Invariance to Computing and System", *International Conference on Mathematics and Computer Science,* 1999.

[15] T. Kalker. G. Depovere, J. Haitsma. M. J. Maes., "Video watermarking systems for broadcast monitoring", *in safekeeping of multimedia contents consultation SPIE Proceedings,* 103—112, 1999.