Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.98 – 103

A Survey: Video Steganography and Security Forbidden Zone and Selective Embedding

K.Maheswari
M.Phil. Scholar,
Department of Computer Science,
Bishop Heber College (Autonomous),
Trichirappalli, Tamilnadu, India

R.Thamarai Selvi
Asst. Professor & Head,
Department of computer Applications,
Bishop Heber College (Autonomous),
Trichirappalli, Tamilnadu, India

ABSTRACT: Steganography is an art of transfer hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. In the recent years, there are lots of systems are introduced. The people invented a huge thing to protect the data and there are lots of hidings techniques are to be invented for security purpose. But that techniques can be hacked by unauthorized users is drawback in existing systems so a new system proposed information hiding behind the video using forbidden zone and selective embedding. This system makes use of correction ability of copying store codes and advantage of forbidden zone data hiding is used. This system is tested by all types of videos that type of video which help to data hiding like avi , mp4 etc. In this study the encryption and decryption techniques used to security key. Without that key no one can see the unique data. This technique is used to secure the database from illegal and the destructive forces. It has large erasure capability of data hiding.

Keywords: Steganography, RSA, Multiple LSB, Data Hiding, Forbidden Zone, Quantization Index Modulation [QIM], Repeat Accumulate Codes [RA], Selective embedding

I. INTRODUCTION

In today's world the protection of superficial data is one of the most serious concerns for groups and their clients with developing monitor compressions, is making company to care for the integrity, confidentiality and safety of critical in sequence. As a result Digital Watermarking is evolving as the foundation for innovativeness data security and compliance, and fast suitable the foundation of security best practice. Digital Watermarking, once seen as a focused, obscure correction of data protection, is lastly coming would dispute that Digital Watermarking and encryption are new knowledge. It was correct times ago and it is quiet true today encryption is the most consistent way to protected data. National security agencies and main financial foundations have long secure their sensitive data using Digital Watermarking & encryption.

Currently the use of encryption is developing fast, being arranged in a much broader set of industry zones and across an increasing range of application and platform. Set purely, Digital Watermarking and encryption have become one of the newest tools in the IT security business the contest now is to guarantee that IT groups are prepared to handle this alteration and are laying the preliminaries today to fulfill their future need. So that the new technology are used to defend the data i.e. watermarking & encryption, decryption. The Forbidden Zone is used to modification is allow while data hiding. Selective Surrounding is utilized in the planned method to define host signal samples fitting for data hiding. It also used for temporal Synchronization for frame drop and insert attack. The density, H.264, frame rate conversions and other hiding methods used.

Cryptography is the apply and study of technique for secure message in the presence of third parties (called adversaries). More normally, it is about constructing and evaluating protocols that overcome the influence of adversaries and which are related to various aspects in data security such as data concealment, data integrity, authentication, and non-repudiation.

1.1 Symmetric-key cryptography

1. Advanced Encryption Standard:-

AES is based on a plan principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its precursor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed chunk size of 128 bits, and a key size of 128, 192, or 256 bits.

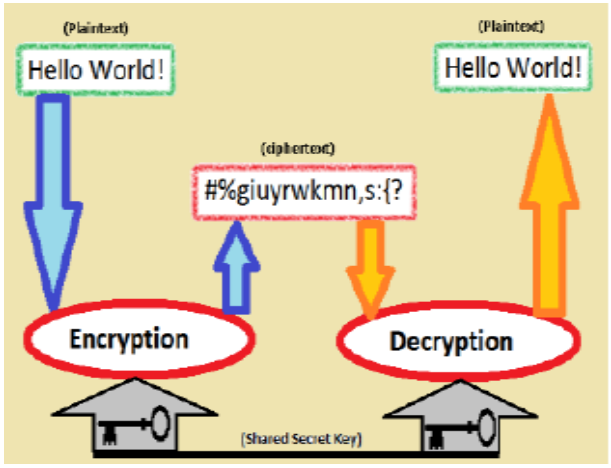


Fig.1 Cryptography Mechanism

2. Data Encryption Standard:-

DES is the archetypal chunk cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a sequence of complex operations into another cipher text bit string of the same length. In the case of DES, the chunk size is 64 bits. DES also uses a key to customize the transformation, so that decryption can allegedly only be perform by those who know the particular key used to encrypt.

1.2 Public-key cryptography

Public-key cryptography, as well known as asymmetric cryptography, refers to a cryptographic algorithm which require two separate keys, one of which is *stealthy*(or *private*) and one of which is *public*. Although different, the 2 parts of this key pair are mathematically linked.

1.3 Steganography

It comes from the Greek word steganos which exactly means "covered" and graphic which means "writing", i.e. enclosed writing. The majority Steganography is the process of covertly embedding information inside a data source without changing its normal use of steganography is to hide a file inside another file.

A. Text steganography:

Hiding in sequence in text is the most important method of steganography. The method was to hide a secret letter in every nth letter of every word of a text message.

B. Audio steganography:

When developing a technique for audio steganography one of the first considerations is the likely environments, the sound signal will travel in environment between encoding and decoding. There are two main areas of modification.

C. Image/Video steganography:

Images are frequently used as the accepted cover objects in steganography. A message is embedded in a digital image through several embedding structures and a secret key. The resulting stego image is sending to the receiver. On the additional, it is processed by the extraction algorithm using the same key.

1.4 Video Steganography with Cryptography

Video Steganography is a technique to hide some kind of files into a carrying Video file. The make use of the video based Steganography can be more capable than other multimedia files, because of its size and memory requirements.

Encrypted Message hide in Video Spatial Domain:-

Least Significant Bit approach is a most accepted approach for hide in spatial domain. In this method, we can take the binary demonstration of the hidden data and overwrite the LSB of each byte within the cover image.

Encrypted Message Hide in Video Frequency Domain:-

Its hide the bits of information in the DCT domain of the stego object. The buried message is a stream of "1"and "0" a total number of 56 bits.

II. RELATED WORK

In today's dynamic and information rich environment, data systems aware become vital for any organization to survive. With the increase in the dependence of the organization on the information system, there exists an opportunity for the competitive organizational and disruptive forces to gain access to other organization in a row system. This hostile surroundings makes information systems security issues critical to an organization. Current info security literature either emphases on random information by describing the record security attacks taking place in the world or it comprises of the technical literature recounting the types of security threats and the possible security systems. In order to secure the communication of data, Steganography has to be implemented. Steganography is the science of devising systems that agree informational to be sent in a safe form in such a way that the only person able to retrieve this information is intended recipient. Traditional techniques i.e. LSB was used image transformation with bit of information. There are several ways of hiding information.

In [3] a steganographic scheme was proposed, it uses human vision sensitivity to hide secret bits. To make this, the top secret data firstly are changed 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 difference of the pixel magnitudes in the host image. A modification to the least significant bit matching (LSBM) steganography was introduced.

This [5] modification provides the desired choice of a binary function of two cover pixels rather than to be arbitrary as in LSBM. To increase the level of security, a combined data encoding and hiding process was proposed.

This [6] process was used to overcome the problem of image color changes after the embedding process. The LSB steganography technique was developed. it based on embedding the secret message into the sharper edge regions of the image to ensure its conflict against image steganalysis based on statistical analysis.

A novel image steganography was suggested in [7], it is based on integer wavelet transform [IWT], it is used to embed multiple secret images and keys in color cover image. A quantization established steganography system presented.

In [11] and [12] two secure communication systems were recommended to be used for voice over IP (VOIP) applications. LSB based steganography was employed to hide the information over an audio protection signal. An extended version of SHA-1 (Secure Hash Algorithm) was introduced in; this system can be used to

encrypt two dimensional data such as image. It is developed to increase the resistance of image based steganography beside the attackers and hackers.

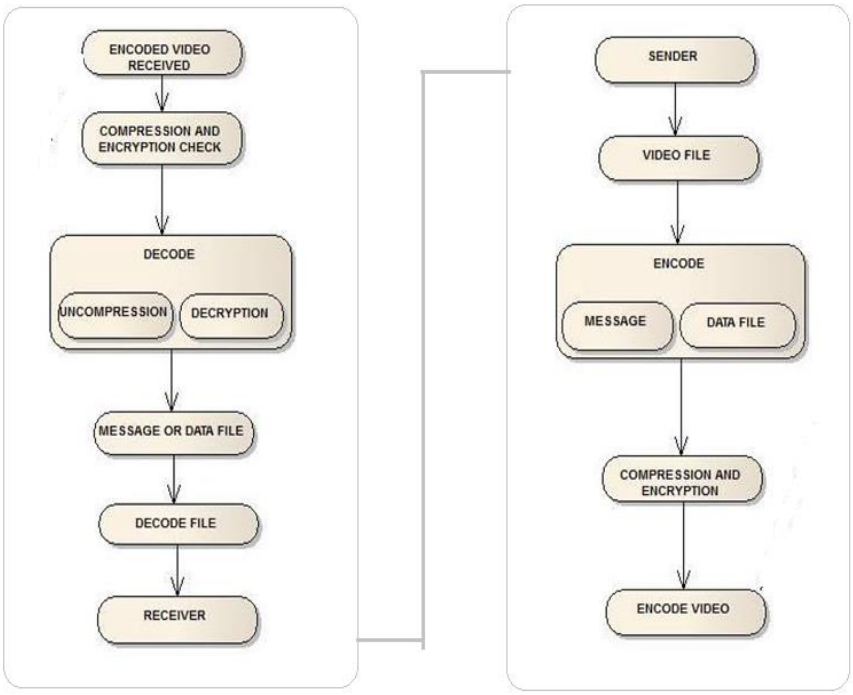
A chaotic signal was employed in [13] for image steganography, which presents a scattering format for the embedded data through the cover image. A high ability and security steganography using discrete wavelet transform (HCSSD) was developed in the wavelet factors for the cover image and the payload image were fused to obtain a single image. All authors in have proposed a two level data security including the text cryptography and image steganography. The secret text is encrypted with Blowfish algorithm followed by embedding it into an image using LSB encoding. The carrier image can be then transmitted over the network.

In [14], authors have suggested an algorithm in which the data is first subjected to encryption consuming Data Encryption Standard (DES). The encrypted message is then passed to embedding phase. In embedding segment the encrypted message will embedded into the cover medium which is either image or audio or video resulting in a stego medium. The embedded stegoaverage contains the encrypted text message which is extracted at the receiver side.

III. PERFORMANCE ANALYSIS

In above existing scheme the steganography data hiding technique used but in this technique the no guaranteed that the data will not fractured is that the future system used. We put forward a block based adaptive video data hiding method that combines FZDH, which is shown to be greater to Quantization Index Modulation QIM & competitive with Decode Quantization Index Modulation DC-QIM , and erasure handling through RA Codes. We utilize selective embedding to conclude which host signal coefficient will be used in data hiding. It is observed that intra and inter frames do not yield significant differences. Thus, in order to overcome local rushes of mistake, we apply 3-D inter leaving which does not make use of selective embedding, but use the whole LL sub band of separate wavelet transform. Furthermore we provide the method with surround synchronization symbols in order to handle frame drop, insert, or repeat attacks. Hence, it can be stated the unique contribution of this paper is to devise a complete video data hiding method that is resistant to de-synchronization due to discriminating embedding and strong to sequential attacks, while making use of the authority of FZDH.

SYSTEM ARCHITECTURE:



Size Comparative Report

We have established the algorithm on various formats and sizes of data and the results are shown in the **Table 1.**

Table 1: Size Analysis Table

S.No	Source File Name	Original Plaint Text(Bytes)	Decrypted Plain Text (Bytes)
1	ABC.txt	48	48
2	School.txt	564	564
3	trs.tif	238543	238543
4	car.jpg	32768	32768
5	thinl.cpp	693	693
6	bear.mp3	8960	8960
7	music.mp3	17360	17360

Time Comparative Report

Table 2, shows the time analysis of the exceeding algorithm, time analysis is performed on the **Table 1** values.

Table 2: Time Analysis Table

Sl. No	File Size (bytes)	Encryption Time	Decryption Time	Encryption / Byte	Decryption / Byte
1	48	0.000565	0.000075	0.00001177	0.00000156
2	564	0.002236	0.000694	0.00000396	0.00000123
3	238543	0.452387	0.359647	0.00000190	0.00000151
4	32768	0.025486	0.017845	0.00000078	0.00000054
5	693	0.005843	0.004127	0.00000843	0.00000596
6	8960	0.065413	0.008413	0.00000730	0.00000094
7	17360	0.235649	0.228631	0.00001357	0.00001317

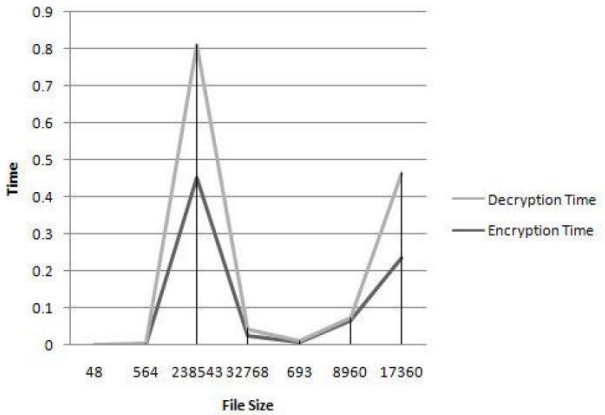


Figure 1: Time Analysis Graph

IV. CONCLUSION

Many Software industries invent Large hiding techniques they examine that not author techniques give the 100% security, filesize 500MB data, lowest level execution time second is result so that in above system we conclude that to generalize the process with video information hiding structure that makes use of erasure modification ability of RA codes and superiority of Forbi. Zone Data Hiding. The method is also robust to frame manipulation attacks via frame synchronization markers. The System can be used to the outcomes specify that the framework can be utilized in video data hiding applications.

REFERENCES

[1] ErsinEsen, A. AydinAlatan,\Robust Video Data Hiding Using ForbiddenZone Data Hiding And Selective Embedding ",IEEE ,VOL. 21, NO. 8,AUGUST 2011

[2] K.Mohan, S.E.Neelakandan \Secured Robust Video Data Hiding UsingSymmetric Encryption Algorithms ", IJIRE ,VOL.6,DECEMBER 2012

[3] R. Ravi Kumar V., Kesav Kumar \Selective Embedding and ForbiddenZone Data Hiding for Strong Video Data Thrashing ",IJETT ,VOL.4,SEPTEMBER 2013

[4] Mr.SudheerAdepu, Mr.P. Ashok ,Dr.C.V.GuruRao \A SecurityMechanism for Video Data hiding " ,IJCTT,VOL.4, August 2013

[5] ResojuOmprakash and D. Jyothi \Block Based Adaptive VideodataHiding Technique", IJMSTH, 2012

[6] Mr. MrithaRamalingam \Stego Machine Video Steganography usingModified LSB Algorithm ", World Academy of Science, Engineering andTechnology,2011

[7] W. Bender D. Gruhl,N. Morimoto,A. Lu, \Techniques for data hiding ",IBM SYSTEMS JOURNAL, VOL.35, NOS 3 and 4, 1996 43.

[8] Tong L.andZheng-ding, Q, (2002), "DWT-based color Images Steganography Scheme", IEEE International Conference on Signal Processing, 2:1568-1571.

[9] Mandal J.K. and Sengupta M., (2010), "Authentication/Secret Message Transformation ThroughWavelet Transform based Subband Image Coding (WTSIC).", Proceedings of InternationalSymposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229.

[10] Septimiu F. M., MirceaVladutiu and Lucian P., (2011),"Secret data communication system usingSteganography, AES and RSA", IEEE 17th International Symposium for Design and Technologyin Electronic Packaging.

[11] H. Tian, K. Zhou, Y. Huang, D. Feng, J. Liu, (2008), "A Covert Communication Model Based onLeast Significant Bits Steganography in Voice over IP", IEEE The 9th International Conference for Young Computer Scientists, pp. 647-652.

[12] Y. Huang, B. Xiao, H. Xiao, (2008), "Implementation of Covert Communication Based onSteganography", IEEE International Conference on Intelligent Information Hiding and MultimediaSignal Processing, pp. 1512-1515.

[13] Cheddad, A, Condell, Joan, Curran, K and McKevitt, Paul,(2008), "Securing Information Content using New Encryption Method and Steganography", IEEE Third International Conference on Digital Information Management.

[14] Rasul E., Saed F. and Hossein S, (2009), " Using the Chaotic Map in Image Steganography", IEEE, International Conference on Signal Processing Systems.

[15] Majunatha R. H. S. and Raja K B, (2010), "High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS),Vol. 3: Issue (6) pp 462-472.

