Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Information Security of Video Steganography Utilizing RSA Algorithm

Sk. Sameerunnisa
Asst. Prof, C.S.E,
Indur College of Engineering,
Siddipet, Hyderabad, India

K. Supriya Suhasini
Asst. Prof, C.S.E,
VBCE,
Nizempet, Hyderabad, India

Shishir Kommu
Asst. Prof, C.S.E,
VBCE,
Nizempet, India

Abstract* — The Steganography and Cryptography systems can be utilized to get security and protection of information. In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Security has turned into a discriminating highlight for flourishing systems and in military alike The steganography is the craft of concealing information inside another information, for example, spread medium by applying diverse steganographic systems. While cryptography brings about making the information human mixed up structure called as figure along these lines cryptography is scrambling of message. Though the steganography brings about misuse of human mindfulness so it stays in secret and undetected or in place. Cryptography and Steganography are remarkable and generally utilized methods that control data (messages) so as to figure or shroud their presence. These methods have numerous applications in software engineering and other related fields: they are utilized to secure military messages, Messages, Visa data, corporate information, individual documents, and so forth. It is conceivable to utilize all document medium, computerized information, or documents as a spread medium in steganography.

***Keywords*-- Steganography, Cryptography, Encryption, RSA,SHA-1.**

I. INTRODUCTION

The Steganography and Cryptography systems can be utilized to get security and protection of information. In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Security has turned into a discriminating highlight for flourishing systems and in military alike The steganography is the craft of concealing information inside another information, for example, spread medium by applying diverse steganographic systems. While cryptography brings about making the information human mixed up structure called as figure along these lines cryptography is scrambling of message. Though the steganography brings about misuse of human mindfulness so it stays in secret and undetected or in place. Cryptography and Steganography are remarkable and generally utilized methods that control data (messages) so as to figure or shroud their presence. These methods have numerous applications in software engineering and other related fields: they are utilized to secure military messages, Messages, Visa data, corporate information, individual documents, and so forth. It is conceivable to utilize all document medium, computerized information, or documents as a spread medium in steganography

Cryptography (from Greek kryptós, "covered up", and gráphein, "to compose") is, customarily, the investigation of method for changing over data from its normal. understandable structure into a limitless arrangement, rendering it confused without mystery learning, the craft of encryption. The craft of ensuring data (plain content) by changing it (scrambling it) into a unreadable. format is called cipher text. Just the individuals who have a mystery key can unravel (or decode) the message into plain content. Scrambled messages can some of the time be broken by cryptanalysis, likewise called code breaking, albeit current cryptography strategies are for all intents and purposes unbreakable. Cryptography scrambles the real message that is being sent. This security instrument utilizes numerical plans and calculations to scramble information into unintelligible content. It must be decoded or unscrambled by the gathering that has the related key [20].

Figure 1.1Cryptographic flow

Generally steganography technique is applied where the cryptography is ineffective [1].

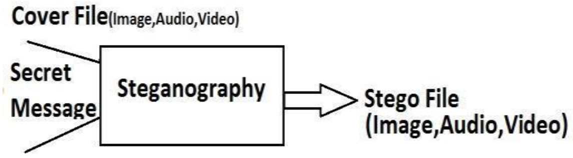

Fig 1: Basic Steganography System

The steganography framework comprises of the spread document (picture, sound, feature and so on) and the mystery message that is covered up inside the spread record by applying steganography the mystery message is concealed and stego record is created which is same as spread picture and go undetected or unaltered. Steganography(fromGreekStegános,"Covered/hidden", and gráphein, "to write") is the art and science of communicating in a way which hides the existence of the communication[1].

Steganography shrouds the very presence of the message by implanting it inside a transporter document of some sort. A busybody can block a cryptographic message, however he may not even realize that a steganographic message exists. Cryptography and Steganography accomplish the same objective through diverse means. Encryption encodes the information so that a unintended beneficiary can't focus its proposed importance. Steganography, conversely endeavors to keep a unintended beneficiary from suspecting that the information is there. [4].Combining encryption with steganography takes into account a superior private correspondence. The objective of steganography is to abstain from attracting suspicion to the transmission of the mystery message. On other hand, steganalysis is a method for distinguishing conceivable mystery correspondence utilizing against steganography. That is, steganalysis endeavors to thrashing steganography methods. It depends on the way that concealing data in advanced media modifies the transporters and presents bizarre marks or some type of debasement that could be misused. Hence, it is vital that a steganography framework to learn that the shrouded messages are not distinguishable[1013 23].

II. RELATED WORK

Steganography incorporates the covering up of media like content, picture, sound, feature records, and so on in another media of same sort or of diverse sort. Later, the message covered up in the chose media is transmitted to beneficiary. At recipient end, opposite procedure is executed to recoup the first message [5].

Some terminologies in Steganography [7]:

Payload**:** The information which is to be concealed.

Carrier File**:** The media where payload has to be hidden.

Stego-Medium**:** The medium in which the information is hidden.

Redundant Bits**:** Pieces of information inside a file which can be overwritten or altered without damaging the file.

Steganalysis**:** The process of detecting hidden information inside of a file.

Stego medium = Payload file + Carrier file.

The four basic techniques used for Steganography are:

Signal & Image Processing:

LSB method: The LSB of carrier medium is directly inserted with the message bit. So LSB of the carrier medium contains the payload

Injection: Concealing information in secti ones of a document that are overlooked by the transforming application. Accordingly abstain from altering those e document bits that are applicable to an end-client leaving the spread record impeccably usable.

Substitution: Substitution of the slightest huge bits of data that focus the important substance of the inception al record with new information in a manner that causes the minimum measure of mutilation.

Generation: : Unlike injection and substitution, this does not require an existing cover file but generates a cover file for the sole purpose of hiding the message. The general form of Steganographic technique is shown in figure 1.2

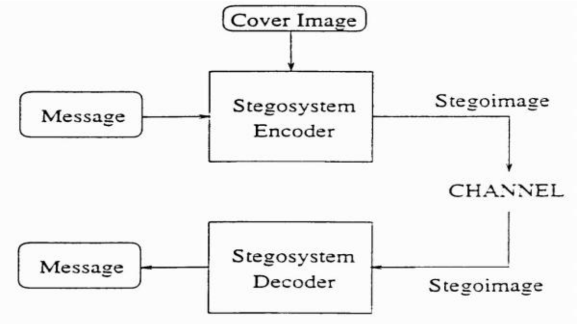

Figure 1.2 Steganographic flow

Many ideas and techniques have been proposed to secure data i.e., mainly concealing of text in images. The simple method to do the same is Least Significant Bit replacement method in steganography. But it has its own limitations [2].Steganalysis can be easily done on LSB replacement technique [19]. The new proposed method overcomes this drawback [12 17 21 22].

Scientists have actualized different methodologies for data and information security to accomplish mystery correspondence. Steganography is a strategy for concealing the mystery messages into the bearer medium, for example, picture, sound, feature and so forth steganography method is for the most part ordered into three principle sorts in particular, technique exploiting image format, method embedding in frequency domain and method in spatial domain[2]. Stego is a Greek word which means hidden. The ancient people used various techniques to send the secret messages during the war time. The evaluation of steganography technique is done with three parameters such as capacity, robustness and security[3]. The system should be capable of hiding the information into cover media, it should be robust to the changes and it should be secured enough from eavesdroppers or attackers that tends to identify or alter the contents of the secret data[4]. The researchers have implemented various approaches depending on the cover medium or the

techniques used such as[27].
a)Cover Generation Method[5]. b)Distortion Technique[6].
c)Statistical Method[7].
d)Spread Spectrum Technique[8]. e)Transform Domain Technique[9]. f)Substitution System[10].
Contingent upon document arranges as spread medium i.e. sound, feature, picture, and content fitting information concealing strategy or application is actualized.

III. STEGANOGRAPHY TECHNIQUES

The effective steganography should have property of remaining intact irrespective of the tampering, the secret message should be invisible and it should go undetected. The capacity of the technique to hide the data should be well achieved

A. Image Steganography

According to computer system an image can be said as array of numbers which represents light intensities at pixels, which results in data. Image is composed of 8 bits per pixel i.e.256 colors.

The colors are generated from three primary colors as RSA has symmetric block cipher and hence uses same red, green and blue (RGB)[28][11-13]. various key for encryption and decryption.

B. Audio Steganography

Audio steganography works by slightly changing the binary sequence and concealing with the secret message. Several methods are proposed such as Least Significant Bit(LSB) replacing last digit of carrier file. Parity coding involves breaking down of signal and then hiding the message in parity bits of each sample. Phase coding involves encoding of secret data to phase shifts. Spread spectrum distributes secret data into frequency spectrum, in which direct sequence and frequency hopping is used. The Echo method generates echo for insertion of secret data into signal[20-26]

C. Video Steganography

The division of feature into sound and pictures or edges brings about the effective technique for information hiding.The utilization of feature records as a transporter medium for steganography is more qualified when contrasted with different techniques.As a consequence of this method is examined and proposed in this paper.

D. Network Steganography

Another methodology for concealing information is to utilize system steganography by sending information with the assistance of system protocol. Network or transport layer, for example, IP/TCP or ICMP and UDP conventions are utilized for sending messages

IV. THE PROPOSED METHOD

The proposed strategy for the information covering up is in view of feature steganography where we have utilized the RSA calculation to make the steganography more secure and robust.The feature steganography is attained to by installing the feature documents with the mystery information that is to be transmitted with the proposition of keeping the mystery information unaltered or stays in place at collectors end.

The calculation was given by three MIT's Rivest, Shamir & Adleman and distributed in year 1977. RSA calculation is a message encryption cryptosystem in which two prime numbers are taken at first and after that the result of these qualities is utilized to make an open and a private key, which is further utilized as a part of encryption and decoding. The RSA calculation could be utilized as a part of blend with Hash-LSB. By utilizing the RSA calculation we are expanding the security to a level above. If there should arise an occurrence of steganalysis just figure content could be removed which is in the encoded structure and is not lucid, thusly will be secure..

RSA algorithm procedure can be illustrated in brief as follows [28]:
(i) Select two large strong prime numbers, p and q. Let n = p q.
(ii) Compute Euler's totient value for n: f (n) = (p - 1) (q - 1).
(iii) Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.
(iv) Calculate a number d such that d = e-1 mod f (n).
(v) Encryption: Given a plain text m satisfying m < n, then the Cipher text c = m^e mod n. Decryption:
(vi) The cipher text is decrypted by m = c^d mod n.

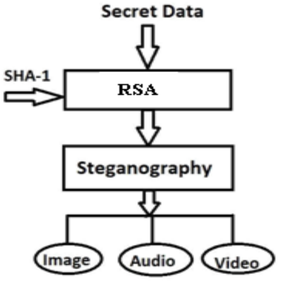

Fig 2:The Proposed Steganography

B. Extraction Of Video File (at Sender Side)

The feature steganography made out of two principle stages specifically extraction of feature documents and inserting of mystery message, as the mystery message is now scrambled utilizing RSA and SHA-1 it can be effortlessly installed into bearer video. The methodology of extraction is indicated in fig.3.The extraction of feature results in casings as feature for the most part made out of still pictures and audio, the sound and picture outlines from the record feature is extracted.From this separated sound the stego document is created as a mystery information is hided in the sound not in the picture frames. Audio contains unused bits or free bits of data in which mystery information can be effectively hided. For making this document more strong against assault or ID stego record is again scrambled utilizing the Propelled Encryption Standard. The stego file generated is then transmitted over the communication channel which remains intact as a result of this complex data hiding method.

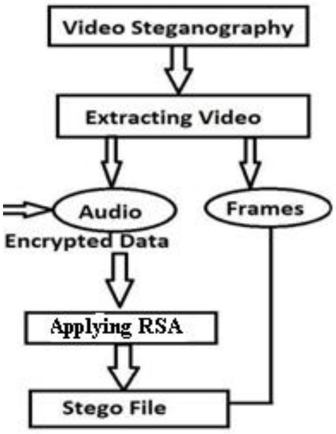

Fig 3: Extraction Of Video at Sender Side

C. Extraction Of Stego File(at Receiver Side)

The stego record can be removed at collectors side by performing decoding of stego document and after that by removing the bearer feature which is only a gathering of sound and picture frames. The resultant information is the scrambled mystery information which is again unscrambled to acquire unique data. Thus the proposed framework gives the most secure methodology utilizing two layer of encryption the first is performed on the mystery information itself and another on the sound document.

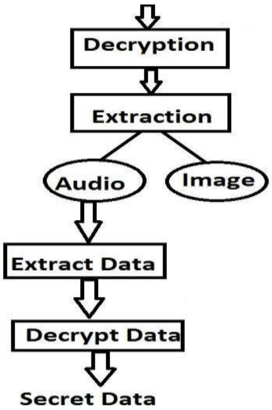

Fig 4: Extraction of Stego File at Receiver Side

V. CONCLUSION

In this paper we displayed a few methods for concealing the mystery information inside the spread medium, for example, image, audio, video. The proposed framework for information concealing uses RSA for encryption and SHA-1 for creating mystery hash capacity or key. Which brings about more secure method for information hiding. We can infer that the proposed framework is more powerful for mystery correspondence over the system channel. A secured Hash based LSB system for picture steganography has been executed. A proficient steganographic system for implanting mystery messages into spread pictures without creating any real changes has been fulfilled through Hash-LSB strategy.

In this work, another method for concealing data in a picture with less variety in picture bits have been made, which makes our strategy secure and more productive.

This method additionally applies a cryptographic system i.e.RSA calculation to secure the mystery message with the goal that it is not simple to break the encryption without the key. RSA calculation itself is exceptionally secure that is the reason we utilized as a part of this system to build the security of the mystery message. A predefined implanting strategy uses hash capacity furthermore give encryption of information uses RSA calculation; makes our method an all that much usable and dependable to send data over any unsecure channel or web. The H-LSB strategy have been connected to .tiff pictures; then again it can work with some other configurations with minor procedural change like for packed pictures.

Execution investigation of the created system have been assessed by contrasting it and basic LSB method, which have come about a decent MSE and PSNR values for the stego pictures. The future degree for the proposed technique may be the improvement of an improved steganography that can have the validation module alongside encryption and unscrambling. In the interim the work can be improved for other information records like feature, audio, content. So also the steganography strategy can be produced for 3D pictures. The further work may contain blend of this system to message processing calculations.

RSA calculation to secure the mystery message with the goal that it is not simple to break the encryption without the key. RSA calculation itself is exceptionally secure that is the reason we utilized as a part of this strategy to build the security of the mystery message. A predetermined installing procedure uses hash capacity furthermore give encryption of information uses RSA calculation; makes our method an all that much usable and reliable to send data over any unsecure channel or web.

The H-LSB method have been connected to .tiff pictures; nonetheless it can work with whatever other arrangements with minor procedural change like for packed pictures. Execution investigation of the created system have been assessed by contrasting it and straightforward LSB method, which have come about a decent MSE and PSNR values for the stego pictures. The future extension for the proposed technique may be the advancement of an upgraded steganography that can have the verification module alongside encryption and decoding. Then the work can be improved for other information documents like feature, audio, content. Additionally the steganography strategy can be created for 3D pictures. The further work may contain mix of this system to
message processing calculations.

REFERENCES

[1] Nutzinger,M.C.Fabian, and M.Marschalek. ”Secure Hybrid Spread Spectrum System for Steganography in Auditive Media”. In Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP), 2010 Sixth International Conference.

[2] Abbas Cheddad,Joan Condell,Kevin Curran,Paul Kevitt,”Enhancing Steganography In Digital Images”.Proc.Canadian Conference on Computer and Robot Vision.

[3] B.Dunbar.A Detailed look at steganographic techniques and their use in an Open-Systems Environment,Sans Institute,1(2002).

[4] Alain,C.Brainos,”A study of Steganography and Art Of Hiding Information,”East Carolina University.

[5] Bender,W,Grulh,D,Morimoto,N. & Lu,A.,”Techniques for Data Hiding”,IBM Systems Journal,Vol 35,1996.

[6] Dunbar,B.,”Steganography Techniques and their use in an Open-Systems environment”,SANS Institute,January 2002.

[7] Marvel,L.,M.,Boncelet Jr.,C.G.& Retter,C.,”Spread Spectrum Steganography”,IEEE Transactions on Image Processing,1999.

[8] Wang,H & Wang,S,”Cyber Warfare:Steganography vs. Steganalysis”,Communications of the ACM,47:10,October 2004.

[9] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking,Artech House, Boston.London,2000.

[10] Jamil,T.,”Steganography:The art of Hiding Information is Plain Sight”,IEEE Potentials,18:01,1999.

[11] B.Pfitzmann,”Information Hiding Terminology,”proc.First Int’l Workshop Information Hiding,Lecturer Notes in Computer Science No.1,174,Spring –Verlag,Berlin,1996,pp.347-356.

[12] Yeuan-Kuen Leea and Ling-Hwei Cheng,”High capacity steganographic model”,IEEE Proc.Visual Image Signal Process.,Vol.147,No.3,June 2000.

[13] Ross J.Anderson,Fabien A.P.Petitcols,on The limits of steganography,IEEE Journal of Selected Areas in Communication,16(4);474-481,May 1998.

[14] M.Ashourian,R.C. Jain,and Y.H.Ho,Dithered Quantization for Image Data Hiding In DCT domain,Proc.of IST2003,2003,171-175.

[15] C.C.lin,P.F.Shiu,High Capacity Data Hiding scheme for DCT-based images.Journal of Information Hiding and Multimedia Signal Processing,1(3),2010,314-323.

[16] A.Nag,S.Biswas,D.Sarkar,P.Sarkar,A Novel Technique for Image Steganography based on Block-DCT and Huffman Encoding,International Journal of Computer Science and Information Technology.

[17] C.C.Chang,C.C.Lin,C.S.Tseng,and W.L.Tai Reversible hiding in DCT-based Compressed Images,Information Sciences Journal,177(13),2007,2768-2786.

[18] C.C.Chang,C.C.Lin,C.S.Tseng,and W.L.Tai Reversible hiding in DCT-based Compressed Images,Information Sciences M.Iwata,k.miyake,A. Shiozaki,Digital Steganography utilizing Features of JPEG Images,IEICE Trans.Fundamentals,E87-A,2004,929-936.

[19] C.C. Chang,T.S.Chen,and L.Z. Chung,A Steganographic Method Based Upon JPEG quantization table modification,Information Sciences Journal,2002,141(1,2),123-138.

[20] Kumar.B.,D.,Bhattacharya,P.Das,D.Ganguly and S.Mukherjee,” A tutorial review on Steganography”,International Conference on Contemporary Computing (IC3-2008),Noida,India,August 7-9,2008,pp.105-114.

[21] Shahereza,S.S. and M.T.M. Shalmani.High capacity error free wavelet Domain Speech Steganography. In Acoustics,Speech and Signal Processing,2008.ICASSP 2008.IEEE International Conference on.2008.

[22] Vapnik,V.N.”Statistical Learning Theory”.John Wiley and Sons,New York,USA,1998.

[23] Johnson,N.F. and S. Jajodia,Exploring Steganography:Seeing the unseen.

[24] Bender,W.W.Butera,D.Gruhl,R.Hwang,F.J.Paiz,S.Pogreb,”Techni ques for data hiding”,IBM Systems Journal,Volume 39,Issue 3-4,July 2000,pp.547-568.

[25] Chiungy,.W.and W. Quincy.”Information Hiding in Real Time VoIP Streams”.in Multimedia,2007.ISM 2007.Ninth IEEE International Symposium on.2007.

[26] Bhattacharya,D.et al.,Hiding Data in Audio Signal.Advanced Communication and Networking,C.,C.,Chang,et al.,Editors.2010,Springer Berlin Heidelberg.p.23-29.

[27] Dipti Kapoor Sarmah, Neha Bajpai.”Proposed System for data hiding using Cryptography and Steganography”.Proc.International Journal of Computer Applications,Vol 9,Isuue2,2010.

[28] H.Al-Barhmtoshy,E.Osman and M.Ezzat.”A Novel Security Model Combining Cryptography and Steganography”. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain “*A New Approach for LSB Based Image Steganography using Secret Key*”, International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[29] Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, “*Hash Based Least Significant Bit Technique for Video Steganography (HLSB)*”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[30] Mamta Juneja, Parvinder Singh Sandhu, “*Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption*”, International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

[31] Swati Tiwari, R. P. Mahajan, “*A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion*”, International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[32] N. F. Johnson, S. Jajodia, "*Steganography: seeing the unseen*”, IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.

[33] Wien Hong, Tung-Shou Chen, “*A Novel Data Embedding Method Using Adaptive Pixel Pair Matching”,* IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.

[34] Amr A. Hanafy, Gouda I. Salama, Yahya Z. Mohasseb, “*A Secure Covert Communication Model Based on Video Steganography*”, Military Communications Conference, IEEE, Pages No. 1 – 6, 16-19 Nov., 2008.
R. Chandramouli, N. Memon, “*Analysis of LSB based image Steganography techniques”,* International Conference on Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.

[35] Weiqi Luo, Fangjun Huang, Jiwu Huang, “*Edge Adaptive Image Steganography Based on LSB Matching Revisited*”,IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 –214, June, 2010.