ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

An Adaptive Study for Different Methodology for Information Hiding

Nagesh Sharma[1], Narendra Kumar Upadhyay[2], Nirmal Kumar Saraswat[3]

Assistant Professor, Dept. of MCA, HIMT Greater Noida, India [1]

Head, Department of Computer Applications, HIMT Greater Noida, India [2]

Assistant Professor, Dept. of MCA, HIMT Greater Noida, India [3]

ABSTRACT: This paper focuses on different terminologies and methodologies for information hiding. To ensure the information so it can be conveyed over the web without being error inclined and harmed has prompted the idea of information hiding data can be hidden in computerized sound, video, and pictures. There are numerous procedures proposed for data covering up as of late, for example, Steganography, advanced watermarking and cryptography. In this paper, we have survey the different data hiding terminologies that utilizations and provide the comparative results. Steganography as the principle key part, we will likewise think about the working of the different calculations. We will attempt to find the inadequacy of the flow methodologies and set the patterns for new research around there.

KEYWORDS: Information hiding, Steganography, Cryptography

I. INTRODUCTION

As of late, there has been an extraordinary development in rapid PC system and sight and sound innovation including picture, sound, video, and all the more particularly internet. Presently a day's computerized correspondence turns into a basic piece of framework, a considerable measure of use are web based and it is imperative that correspondence made the mystery to shield it from meddlers and assaults. For secure correspondence different procedures have been proposed in the past, for example, cryptography, advanced watermarking, Steganography and so on.

The word Steganography originates from Greek word stegano which implies secured and Graphic implies composing. Steganography is the craftsmanship in which the presence of correspondence is covered up. It is the specialty of concealing the way that correspondence is going on. In traditional Steganography procedures, the framework utilized for encoding information has kept the mystery. In any case, present day Steganography is perceivable just if the mystery key is known. Steganography and cryptography are regularly confounded in light of the fact that they are comparable methodologies for concealing data [1], yet there is a critical distinction between the two. In Steganography data is shrouded so it creates the impression that no data is covered up by any stretch of the imagination. In the event, that client's view a question in which data is shrouded they will have no.

clue that data is covered up in the protest thus no endeavors will be made to unscramble the data [2]. In Steganography the genuine data that will be covered up is not kept in its unique frame but rather is changing over into an option comparable interactive media record like the picture, video, sound. This option document is covered up inside another protest; this message is sent to the beneficiary over the system. At the accepting sides, the genuine messages decoded. Contingent upon the idea of cover question Steganography can be separated in to five sorts.

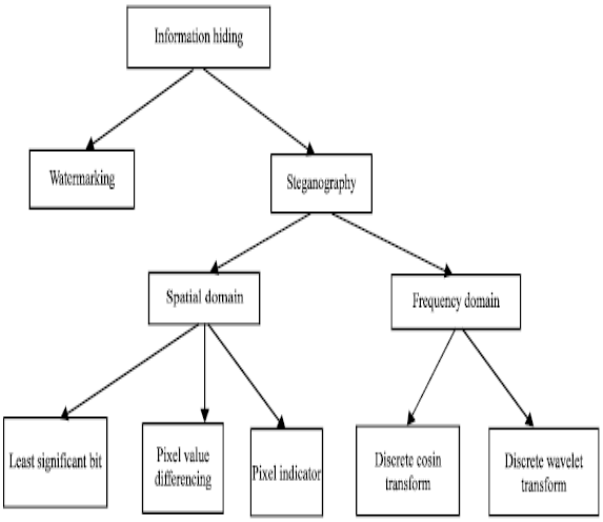
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017



1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Protocol Steganography

With the advances in the field of communication it become easier to decrypt cipher text, hence more sophisticated techniques were needed which led to discovery of Steganography. As of late, there has been an extraordinary development in rapid PC system and sight and sound innovation including picture, sound, video, and all the more particularly internet. Presently a day's computerized correspondence turns into a basic piece of framework, a considerable measure of use are web based and it is imperative that correspondence made the mystery to shield it from meddlers and assaults. For secure correspondence different procedures have been proposed in the past, for example, cryptography, advanced watermarking, Steganography and so on.

fig1: Steganography watermaking

The word Steganography originates from Greek word stegano which implies secured and Graphia implies composing. Steganography is the craftsmanship in which the presence of correspondence is covered up. It is the specialty of concealing the way that correspondence is going on. In traditional Steganography procedures, the framework utilized for encoding information has kept the mystery. In any case, present day Steganography is perceivable just if the mystery key is known. Steganography and cryptography are regularly confounded in light of the fact that they are comparable methodologies for concealing data [1], yet there is a critical distinction between the two.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

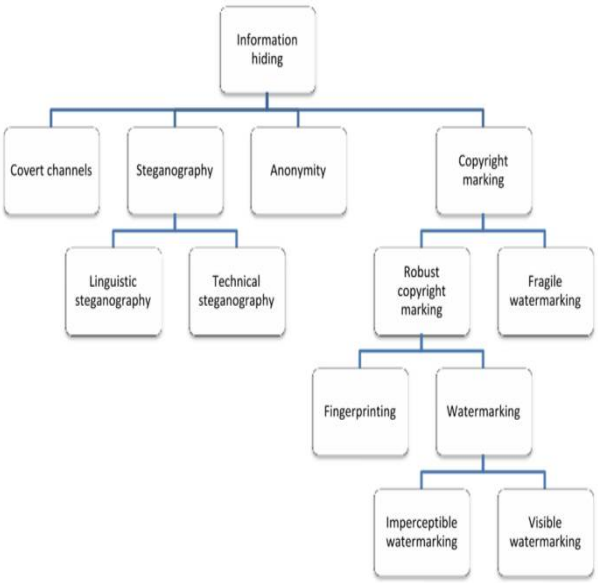
In Steganography data is shrouded so it creates the impression that no data is covered up by any stretch of the imagination. In the event, that client's view a question in which data is shrouded they will have no clue that data is covered up in the protest thus no endeavors will be made to unscramble the data [2]. In Steganography the genuine data that will be covered up is not kept in its unique frame but rather is changing over into an option comparable interactive media record like the picture, video, sound. This option document is covered up inside another protest; this message is sent to the beneficiary over the system. At the accepting sides, the genuine messages decoded. Contingent upon the idea of cover question Steganography can be separated in to five sorts. Watermarking is signal or streams of bits i.e securely and robustly embedded in to original content such as image, video, or audio signal produced a watermarked signal. Watermarking is closely related to a Steganography and mainly used for copyright protection and owner authentication. The process of embedding watermark in to a digital data is called digital watermarking

II. RELATED WORK

The reason for cryptography and Steganography is to give mystery correspondence. However, there is an essential distinction between the apparatuses. The cryptography conceals mystery message from assaults and noxious individuals where as Steganography shrouds the presence of a message. In cryptography when the framework is broken the aggressor can read the mystery message. Yet, in Steganography the aggressor need to recognize that Steganography is been done in a specific protest have the capacity to peruse the installed message, so the breaking of the framework holds distinctive significance for both the data concealing techniques [3].

In cryptography, the message structure is mixed so the message has no significance, and the message can be unscrambled just when the decoding key is accessible. Cryptography gives the data passing component between people such that the outside or assailant can't read the message unless the decoding key is accessible. Cryptography additionally gives confirmation system.

Interestingly Steganography is concealing a mystery message with in a bigger message to the presence of mystery message can't be identified. The question in which a mystery message covered up is called cover picture. A message i.e. changed over into figure content may at times prompt doubt at the less than desirable end while the Steganography strategies make an imperceptible message that will keep an unintended beneficiary from suspecting that the information exists. Cryptography and Steganography can be joined together, messages can be encoded by utilizing cryptography and the scrambled message can be concealed utilizing Steganography. This outcome into a Stego _image which does not uncovers the mystery data and can be transmitted securely.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

III. ATTACKS

There are various attacks that can be used in any cryptographic system; we discuss here a few of them that have significance in Steganograhic systems.

- *Replay attack* – In replay attacks communication stream between two parties is captured by an adversary, and replayed to produce unauthorized effect. As an example consider communication between two parties A and B. A wants to communicate with B, for this B asks for the identity of A. suppose A provides some identity possibly after hash transformation, and eavesdropper C keeping track of the communication stream captures the identity. After the communication between A and B is over C connects with B and when asked for identity provides the same captured password. To avoid replay attacks sessions, one time password, MAC, and time stamping can be used.
- *Forgery Attack*- In forgery attack the original message is captured by the eavesdropper which in turn transmits another message in place of the original one. This way the communication parties are not able to communicate properly.
- *Frame Deletion Attack*- In frame deletion attack, the attacker deletes frame for the original message. The lost message can be recovered at the receiver because each frame contains one alphabet of the message which can be formed by using 26 combinations of the English alphabets and by forming a logical term from the dictionary.
- *Eavesdropping*- An eavesdropper or adversary is a malicious entity whose goal is to prevent the communicating parties from achieving their objectives. An eavesdropper attempts to discover secret data between communicating parties, spoofing the identity of sender or receiver, distorting the transmitted data, sending malicious information in place of original messages

IV. INFORMATION SECURE SCHEME USING VARIOUS TECHNIQUE

Secure data transmission using Steganography [4] an algorithm is designed that uses both cryptography and Steganography. To hide encrypted data TCP/IP header is used as Steganography carrier .To provide secure data transmission when there are large number of users Steganography technique is used . To provide security over network cryptography is used but the third party may detect the secured message.

To hide secret encrypted data identification field of IP header is used, Identification field is used only when fragmentation occurs. At the receiver end, identification field tells the right order for resembling. If there is no fragmentation identification field is not used. MTU (Maximum transfer unit)is used to avoid fragmentation . The packet size for transmission over network is decided by MTU. Sender and receiver both should know the MTU unit. For encryption and decryption Elliptic curve cryptography is used , it is a public key cryptography .In public key cryptography each device taking part has two set of keys public and private and operations associated with it. Only a particular user or device knows the private key, whereas public key is distributed to all the users.

The operation of ECC defined over the elliptic curve is as shown in equation

$$Y= x3 + ax +b, \text{ where } 4a+27b \neq 0$$

Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies this equation plus a point at infinity lies on the elliptic curve. A point in the curve is public key where as any random number can be taken as private key. To obtain the public key private key is multiplied by generator point G in the curve.

A conceptual scheme is proposed for secure file transmission using Steganography. Suppose Alice is sender, and wants to send a secret file to Bob which is at receiver. The propose technique provide a secure system in case of authentication and avoid illegal transmission of secret communication on web.

The propose technique provide a secure system in case of authentication and avoid illegal transmission of secret communication on web.

Motion Vector Techniques [5] - An algorithm is designed for hiding the data in moving object by using motion vector techniques in video Steganography. The art of hiding information so that messages are not revealed is Steganography .Video files can be said as collection of images, so the used for techniques images and audio can be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

applied to video files too. A video is a moving stream of image and provides an advantage that is large amount of data that can be hidden inside it.

A new technique is proposed to hide the data in the moving objects, using the motion vector. The data is encrypted by using the AES algorithm and then hided, to enhance the security of the data. The data is hided in the horizontal and the vertical components of the moving objects. To evaluate quality of video after the data hiding is done, PSNR value is calculated. The algorithm works in five steps viz Video Compression, Motion Vector, Encryption, and Extraction of original data and Calculation of PSNR value.

In Most of the work proposed earlier data were hidden in still images that had to suffer distortion. In this paper for data transmission compressed video is used that can store large volume of data, to show distortion free transmission PSNR value is calculated.

Frame video Watermarking [6]-An algorithm is designed for transmitting the required secret information by embedding the information in to video after encryption using frame video watermarking. A 512 bit key value is used for encryption and positioning of secret information. Security is considered as serious issue to transfer secret information from one point to another securely. The following notations which are used in proposed techniques as follows

T = framing time
n= frame number
a= 128 bits in length
a = t+n
T = t/10,000
b= represents frame component of length 128 bits used to choose one of R,G,B gray level images of chosen frame
c= starting position and 128 bits in length used to compute starting index (si)
d= 128 bits encryption key
t key= key= a*b*c*d
Where a, b, c, d are so chosen that they are relatively prime with each other

In this proposed algorithm it is assumed that watermark is inserted in to video frames where watermark is encrypted message. This technique is described by using predefined framing time T, break the videos in to frames to get total number of frames such as k and choose the frame number using n in which secret message is inserted.
Chosen frame number= (n mod k)
To compute the encrypted message m' using AES- 128 and SHA-512 code for original message where d is used as key for encryption using AES and t key is used as key for generating SHA code. By using variable c the starting index (si) is calculated as si=(c mod(i*j)) and starting from si insert m' linearly in to chosen frame, by using the watermarked frame video is reconstructed. To obtain the extracted message at receiver end, they first break the videos into frames as in proposed algorithm and from the starting position extract the encrypted message and SHA code. The SHA code for decrypted message where decryption process is done by using AES-128. If computed and received SHA code comes equal than received message is valid otherwise it will be rejected. In this article author clearly defined that the peak signal to noise ratio , noise correlation are very good as compared to other techniques and total number of brute force attack required to break the key are very high .

Secure data transmission using video Steganography [7] – An Algorithm is intended to give a productive and secure strategy for video Steganography. In this paper, creator proposed a technique which makes a record of mystery data. Rather than looking the whole video for mystery information from Steganography video, which increments the computational time to the extraction procedure. In this paper, an answer is given to the issue by making a record for mystery data or information which is put away in the video. It diminishes the computational time taken for extricating the procedure. The file is set on an edge of the video itself. They utilize a few edges or picture of the video to conceals the mystery information. Mystery information is put in arbitrary edges. File outline is depicted that give the data about casing which is put on some edge of the video. Record outline contains the mystery data or information. The casings which contain mystery data or edges which don't contain mystery data are both Steganography with some arbitrary information. So this gives extra security to the mystery information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

In this paper, a Steganograhic procedure is utilized which depends on LSB (Least Significant Bit Insertion) technique. The extraction procedure in the Steganograhic video turns around procedure of concealing mystery data into the video.

Secure Communication using symmetric and asymmetric cryptography techniques [8] - In this paper, an Algorithm is intended for secure correspondence utilizing symmetric and asymmetrical cryptographic procedures. An approach is proposed to guarantee safe and secured exchanged of information or data. By utilizing symmetric and hilter kilter cryptographic strategies, satellite based correspondence is a decent technique to transmit computerized data starting with one geographic area then onto the next. Thought (International information encryption algorithm) is utilized uses 128 bits, MD5(Message process calculation) gives 128 bits, and RSA(1024 bit uneven calculation) for data security.

To give secure correspondence following strides are utilized as a part of proposed strategies as takes after:

1. Using MD5 sender creates a 128 piece hash of a message.

2. By utilizing RSA hash esteem is scrambled with sender's private key.

3. An irregular 128 piece session key is picked by the sender and by utilizing IDEA message is scrambled with the session key.

4. With the beneficiaries, the open key session key is encoded and this outcome is sent as figure content to the beneficiary.

5. By utilizing RSA, beneficiary decodes some portion of figure message with his private key to get the session key.

6. By utilizing IDEA remaining piece of figure message is unscrambled with the assistance of session key.

7. By utilizing MD5 beneficiary creates the hash estimation of the message.

8. By utilizing RSA beneficiary unscrambles the computerized signature with sender's open key.

9. By utilizing MD5 hash esteem is created from the outcome

V. SIMULATION RESULTS

We have looked into a considerable measure of methodologies that hide the information safely and try to transmit it securely without interruption. We have found that the methodologies are inclining towards the arbitrariness of the information and secure keys. An absence of outsider confirmation is likewise there. Techniques are extremely mind boggling and can't be utilized for continuous methodologies. Some may fall flat against assaults like Replay attack, Forgery attack, Frame erasure attacks, eavesdropping. So there is a great deal of extension here to accomplish better security of information.

VI. CONCLUSION AND FUTURE WORK

We have given review analysis of several methods for information hiding along with their Algorithm analysis and different approaches. Steganography was utilized to pass the execution design of the 9/11 WTC attack. Hence, through this paper, we have recently attempted to make mindfulness and set up the way that such strategies do exist. Still, inquires about are in advance everywhere throughout the world in this creative field of Steganography, remembering the positive effects of this on the general public in the present ICT based progressive age of 21st century.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

REFERENCES

[1] R.Chandramouli and N.D.Memon, Steganogrphy Capacity: A Steganalysis Perspective
[2] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly , Swarnendu Mukherjee and Poulami Das, A Tutorial Review on Steganography
[3] M.M. Amin, M.Salleh, S.Ibrahim, et al, "Information hiding Using Steganography", 4th national conference on Telecommunication Technology Proceedings(NCTT 2003) ShahAlam, Malaysia, pp. 21-25, January 14-15,2003
[4] R.M.Goudar,PrashantN.Patil, Aniket G.Meshram,Sanyog M.Yewale,Abhay V.Fegade, "Secure Data Transmission by using Steganography," *Information and Knowledge Management Vol2,No.1,2012*.
[5] P.Paulpandi, Dr.T.Meyyappan: Hiding Messages Using Motion Vector Technique In Video Steganography, International Journal of Engineering Trends and Technology- Volume3Issue3-2012.
[6] Lovelesh Saxena, Anuj Tewari, k.V.Arya ,A Novel Technique for Secure Information Transmission using Framed Video Watermarking, in: Springer 2011
[7] R.Balaji ,G.Naveen.: Secure Data Transmission Using Video Steganography , IEEE 2011
[8] Omar M.Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik, MV Ramana Murthy, "Secure Communication Using Symmetric and Asymmetric Cryptographic Techniques," I.J. Information Engineering and Electronics Business, 2012, 2, 36-42.