REVIEW ON INFORMATION HIDING TECHNIQUES: A COMPARATIVE ANALYSIS

A.Anuradha[1], Hardik B. Pandit[2]

[1]*L.J.Institute of Computer Applications, Ahmadabad*
anuradha.acharya77@gmail.com
[2]*Department of Computer Science, Sardar Patel University, Vallabhvidyanagar*
hardik00@gmail.com

Abstract

IT revolution along with the industry revolution, gave birth to some modern technologies like internet, web technology, and cloud computing. Among these, cloud computing is the most advanced technology of sharing resources, which have deeply impacted our social life, work culture and privacy. Besides the positive aspects of these growing technologies, the negative impact must be given a second look. All industrial and social dealings are almost completely dependent on the cyber space which can be exploited easily because everything is open and there is lack of security in it. Hence the data exchanged through the communication channels, as well as the data residing in the remote storage spaces provided by the third party service providers, is under threat. Thus the cyber space which is the fifth domain according to modern view is to be protected after the other domains:land, sea, air and space, for developing and retaining the confidence and faith of its users. Different approaches have been proposed by several researchers for enhancing this security issue thorough various information hiding techniques. The latest technologies being used are cryptography, watermarking and steganography. Along with different cryptographic and watermarking techniques, a variety of steganographictechniques also havebeen used for secure transmission of data. Among which image steganography has been proved to have better features in terms of security, capacity, robustness and integrity than the other types. Thepaper focuses on these existing technologies andcompared them all on various aspects, to give an overview on the Security Zone in the web and its journey.

Keywords*: Cryptography, Watermarking, Steganography, Information Security.*

----------***----------

1. INTRODUCTION

In this modern era, both industry and the social life has been dependent completely on internet and computing, in short on what is called the information technology, which has definitely made our life more comfortable and dynamic[1]. However existence of vulnerabilities in the system has created some security issues which has greatly affected the privacy of individuals [2, 6, 8, 11]. Lots of transactions require sharingthe private data with the third parties which makes it insecure breaking the trust level of IT users. Thus data in communication channels as well as the data being shared with any other party is open to be accessed by invaders because of the breach holes in the system [5].This dependency on the third party must be taken care of to rebuild the trust level of its users [1, 2, 10]. The latest technology of cloud computing, wherethe approach is to share computational resources is also facing such security issues [3, 5] and the problem needs to be resolved.

These security issues has become an eye catching research area for the modern researchers [2, 18].Great many ideas and technologies have been proposed by many for removing the problem of insecurity [4, 19]and still it has become the hot research area in the advanced technologies like cloud computing[6].

The attempt made was either to securely transmit the concerned data either by making it illegible or unreadable through encoding or masking[11]. The idea was to hide the presence of secret data or to make it unreadable.
A brief overview and their comparison can through some light for further research in this respect.

2. INFORMATION HIDING TECHNIQUES: CLASSIFICATION

The solution for maintaining the secrecy of data can have two approaches:

- Information hiding
- Cryptography

In cryptography the message is encoded. Thus it is difficult to get the original message by decoding it without knowing the encoded method. However it can be known that the message has been encoded.

But the concept of information hiding is that, the presence of secret message cannot be known. It is the process in which the data is not visible to the common human man eye or ear, thus no doubt can be generated for the hackers. The classification can be visualized by the figure 1.

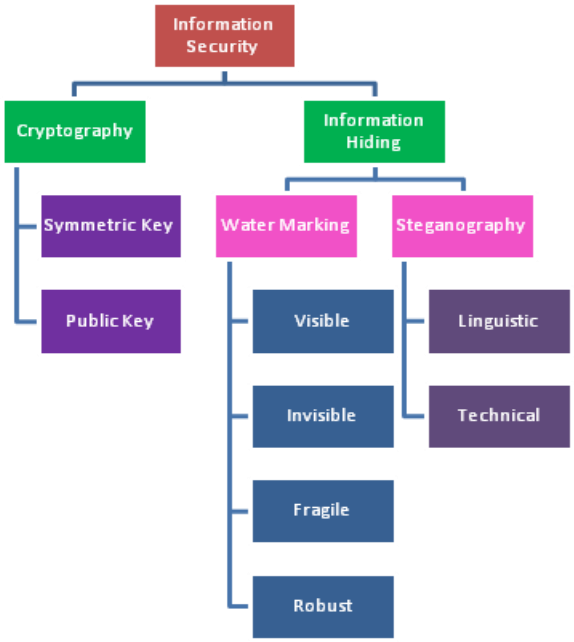

Figure 1: Classification of Information Hiding Techniques

Information hiding can be done either by watermarking or steganography. Thus the techniques that have been implemented yet are:

- Cryptography
- Watermarking
- Steganography

- **Cryptography**is the process of encrypting the data or converting the original data into ciphers by using some keys and encrypting algorithms so that the original data is not readable by the intruders, making it difficult for them to extract the original data.
- **Watermarking**is the process of embedding a bit pattern as a part of the identification, into a carrier signal like image, audio or video file for proving the ownership of the original information. Both visible and invisible watermarking are used for authentication.
- **Steganography**is the process of concealing the file, image or video in another message, file,audio or video in such a way that its presence cannot be detected by the intruders. Only the intended recipient can know the very existence of the message.
- All these technologies either used separately or combined, so as to get the best way of concealing the data and to protect it from any kind of existing and feasible attacks. A great many ideas have been proposed and somewhat different approach of these techniques have been used for better results.

3. STEGANOGRAPHY: AN OUTLINE

Steganogrphy is the concept of hiding the secret message in a cover by embedding the message bits in the cover image. It is derived from the Greek word steganos or "covered", "concealed" or "protected" and graphie or "writing". Thus any message audio or video can be concealed within another file message, audio or video. This concept can be further stepped ahead by combining it with cryptography for protecting the data with higher security [14, 16]. Besides this, watermarking is also being used rigorously, as a part of secure transmission of data, protecting the authentication of the original data [19]. Further digital watermarking can be visible or invisible. In visible watermarking the hiding information representing the authenticity or the ownership of the digital image is visible, whereas, it is invisible in the second type.

Thus invisible watermarking is a type of steganography but it can be retrieved easily by various means. So, sending of information representing the ownership of the image, video or pictures is the concept of digital watermarking and the process of changing the digital image in such a way that, only the sender and the intended recipient can only detect the hidden message is the concept of steganography. But cryptography makes the contents unreadable or illegible, though the encoded message can be seen or it can be known that the data has been encoded. In steganography the presence of the secret message is unseen or undetectable by the attackers which make it the most advantageous technique to be used for concealing the secret message from the intruders or eavesdroppers. Further steganography can be Text, Audio, video, digital and network protocol based, as shown in figure 2.

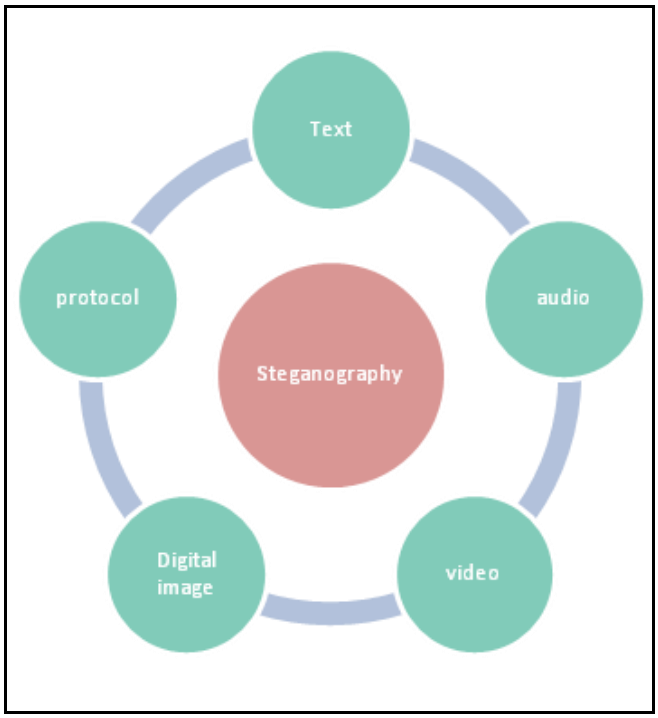

Figure2: Types of Staganography

Among all these types digital steganography has been proved to the most robust technique in terms of capacity, robustness and imperceptibility. At last it can be quoted that steganography provides the security, anonymity and privacy of data, thus becoming the robust technology being used in this digital era.

4. A COMPARATIVE STUDY OF CRYPTOGRAPHY, WATERMARKING AND STEGANOGRAPHY

5. CRYPTOGRAPHY

Advantages

[1]. To keep the data private, and it is difficult for the destructor to read it, until it is decoded.
[2]. It is very difficult for the intruder to find out the key for the decoding.

Disadvantages:

[1]. It involves a lengthy process and little bit time consuming for:
[2]. Creating the code (Encryption)
[3]. To extract the code (Decryption)
[4]. Difficult to generate the key.
[5]. More complicated in terms of lots of concepts like public key, private key, symmetric and non- symmetric keys.

Watermarking

Advantages

[1]. To authenticate the ownership. It is easy to know if any tampering is there.
[2]. It is somewhat easy method.

Disadvantages

[1]. May distract the image.
[2]. The data will become unreadable if it is compressed, or resized.
[3]. Oversized watermarks may hide the image clarity.
[4]. Small watermarks are easily removable. Using clone or trimming tools, the watermark can be removed.

STEGANOGRAPHY

Advantages:

[1]. Hidden information is not detectable.
[2]. More secure than cryptography and watermarking.
[3]. Insertion and extraction mechanisms are only known to the sender and receiver through symmetric keys.
[4]. The detection is difficult.
[5]. Does not alter the structure of the secret message.

Disadvantages:

[1]. It is a tedious job, if the size of the document to be sent is large.
[2]. Once the existence of embedded data is known somehow, then it is difficult to protect the data.

A big question mark is which among all these techniques can provide the best security. A comparative analysis of all these techniques may provide a better way to deal with this problem of security as in the following table.

Table 1 shows comparative analysis of the information hiding techniques.

Table-1 Comparative analysis of the information hiding techniques

Subject	Water marking	Cryptography	Steganography
Goal	To protect the carrier	To make the contents unreadable	To protect the secret information
Usage	Copyright protection, annotation of photographs, source tracking	Electronic money transfer, Time stamping, Authentication and digital signatures	Modern printers, terrorists, intelligence services
Secrecy	Visible or invisible based on the requirement	Encoded text is illegible or unreadable	Invisible to unaware observer
Job type	Somewhat easier	Complicated in terms of concepts like public key, private key and symmetric key	Tedious job
Cover type	Cover choice is restricted	N/A	Any cover can work
Robustness	Less	Less	More
Imperceptibility	Can be removed	Can be deciphered	Undetectable
Key used	Not required	Key is required	No key, Public key or secret key
Threats	Image processing	Cryptanalysis	Steganalysis

The table clearly indicates that, steganography is stronger than watermarking and cryptography. Further seeing the disadvantages of it, it is required to have more research in this area so as to make it the most robust technique for protecting the concerned data from hackers.

6. CONCLUSION

From the comparative analysis of the information hiding techniques, it is definitely indicated that steganography can be the more effective approach in protecting the data with the idea of secretly transmitting it without creating any doubt on the part of the attackers. Since there is no restriction on the type of the cover to be used for concealing of the secret message, it would be more flexible too. On the other side image steganography has been proved to have better features in terms of security, capacity, robustness and integrity than the other types. But there is always the risk of steganalysis attacks. Thus a more robust technique can be implemented by analyzing the existing techniques of steganography and steganalysis, comparing all of them in terms of some important factors affecting their overall performance, and modeling a more qualified algorithm in fulfilling the goal of secure transmission of data. The steganography can be accompanied with encryption techniques for more fruitful results and thus an attempt can be made to regain the trustof the web and cloud users, and helping them to avail the services in a superior way.

REFERENCES

[1]. Waman S Jawadekar, Management and IT Consultant, Management Information Systems,Text & Cases, A Digital-firm Perspective, 4th Edition, Tata McGraw Hill Education Private Limited, New Delhi.

[2]. Swapna Lia Anil, RoshniThanka**, "**A Survey on Security of Data outsourcing in Cloud**",** ISSN2250-3153**,**International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.

[3]. Devanshu Tiwari, Assit. Prof. Damodar Tiwari, "A survey of cloud computing security threats", International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV.

[4]. Mr.K.Sriram,Ms.N.Radhika**,** "a scalable and secure sharing of phr in cloud computing"**,** International Journal of Computer Science and Mobile Applications, ISSN: 2321-8363,Vol.2

[5]. Issue.3, March- 2014, pg.35-41.

[6]. KallimullahLone, Md. Ataullah, "A Review on Cloud Computing Privacy Solutions",

[7]. International Journal of Advanced Research in Computer Science and Software Engineering,ISSN: 2277 128X,Volume 3, Issue 2, February 2013.

[8]. G.Kalpana, P.V. Kumar and R.V.Krishnaiah, **"**A brief Survey on Security Issues in Cloud and itsServicemodels", International Journal of Advanced Research in Computer andCommunication Engineering,Vol. 4, Issue 6, June 2015.

[9]. S.Sudha, V.Madhu, Viswanatham, "Addressing security and privacy issues in cloud computing", Issn: 1992-8645, E-Issn: 1817-3195,20thfebruary 2013. Vol. 48 no.2.

[10]. Keiko Hashizume,David G Rosado,EduardoFernández-Medina and Eduardo B Fernandez, "Ananalysisof security issues for cloud computing", Hashizume et al. Journal of Internet Services

[11]. and Applications 2013, 4:5.

[12]. Vishnu Patidar, MakhanKumbhkar, "Analysis of Cloud Computing Security Issues in Software as a Service", International Journal of Scientific Research in Computer Science and Engineering, ISSN: 2320-7639, Volume-2, Issue-3 30 Jun 2014.

[13]. Abraham E. Eviwiekpaefe, FiyinfoluwaAjakaiye, "The trend and challenges of cloud computing: a literature review", International Letters of Social and Humanistic Sciences Vol. 16 (2014) pp 13-20.

[14]. Dr.P.K.Rai, R.K.Bunkar, "Study of Security Risk and Vulnerabilities of Cloud Computing",International Journal of Computer Science and Mobile Computing (IJCSMC), ISSN 2320– 088X, Vol.3, Issue. 2, February 2014, pg.490 – 496.

[15]. Ms. Disha H. Parekh, Dr. R. Sridaran, "An Analysis of Security Challenges in Cloud

[16]. Computing", IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 4, No.1, 2013

[17]. W.SharonInbarani, C.Kumar Charlie Paul, W.Andrew Jerome Jeevakumar, "A Survey on

[18]. Security Threats and Vulnerabilities in Cloud Computing", ISSN 2229-5518, International

[19]. Journal of Scientific & Engineering Research, Volume 4, Issue 3, March -2013.

[20]. MohitMarwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy In Cloud Computing", ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[21]. Miss. Pallavi A. Patil, Prof. K. G. Bagde, "Cloud Computing and Faults in Cloud Computing",International Journal of Computer Science and Mobile Computing (IJCSMC), ISSN 2320–088X, Vol. 3, Issue. 5, May 2014, pg.415 – 421.

[22]. Muhammad AdeelJavaid**, "**Cloud Computing Security and Privacy**",** Computer Science and Information Technology 2(5): 219-231, 2014.

[23]. Rajesh Kumar, A.J. Singh**, "**Understanding Steganography over Cryptography and Various Steganography Techniques", IJCSMC, ISSN 2320–088X, Vol. 4, Issue. 3, March 2015, pg.253 –258.

[24]. Karun Handa, Uma Singh**, "**Data Security in Cloud Computing using Encryption and

[25]. Steganography**",** IJCSMC, ISSN 2320–088X, Vol. 4, Issue. 5, May 2015, pg.786 – 791.

[26]. Richa Dubey, ApurvaSaxena, Sunita Gond, "An Innovative Data Security Techniques UsingCryptography and Steganographic Techniques", (IJCSIT) International Journal of Computer Science and Information Technologies,

ISSN: 0975-9646, Vol. 6 (3), 2015, 2175-2182.
[27]. SudiptaSahana, MadhusreeMajumdar, Shiladitya Bose, AnayGhoshal, "Security
[28]. Enhancement Approach for Data Transfer Using Elliptic Curve Cryptography and Image
[29]. Steganography",International Journal of Advanced Research in Computer and
[30]. Communication Engineering, ISSNOnline) 2278-1021 ISSN (Print) 2319-5940 Vol. 4, Issue 4, April 2015.
[31]. V. Spoorthy, M. Mamatha, B. Santhosh Kumar**, "**A Survey on Data Storage and Security in Cloud Computing**"**, International Journal of Computer Science and Mobile Computing, ISSN 2320–088X**,** Vol. 3, Issue. 6, June 2014, pg.306 – 313.
[32]. Varsha Yadav, PreetiAggarwaal**, "**A Survey on Security in Cloud Computing**",** IJCSMC, ISSN 2320–088X, Vol. 3, Issue. 4, April 2014, pg.509 – 513.