3rd National Conference on Green Technology and Science for Sustainable Development
© 2020 IJSRST | Volume 5 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
International Journal of Scientific Research in Science and Technology

A Survey on Image Security

Sarita T. Sawale, Devika M. Gaikwad, Rachana N. Khadse
Information Technology, Anuradha Engineering College, Chikhali, Maharashtra, India

ABSTRACT

Due to increase use of internet we required techniques for the protection of channel. The security of secret information can be provided using steganography, cryptography, watermarking and morphing. Steganography refer to the practice of concealing the message in the manner in which it will do no meaning other than intended recipient and encryption of other hand. Steganography hide the secret message while cryptography changes message format itself. Watermarking is the process of hiding digital information in carrier signal. In the process of morphing source image is gradually distorted and disappeared while producing the target image. So, this paper covers the overview of methods for image security, need of image security and its comparison.

Keywords : Security, Cryptography, Steganography, Visual Cryptography, Watermarking.

I. INTRODUCTION

The image is mostly used communication mode in the different areas like medical area, research area, business area, military area etc. [1]. The security of information feels to be important to an organization was provide primarily by physical and administrative means [2]. In today's rapid the image is mostly used communication mode in the different areas like medical area, research area, business area, military area etc. The security of information felt to be valuable to an organization was provide mainly by physical and administrative means. In today's rapid growth of digital communication and electronic data exchange, many of us communicate in resources cyber space without thinking about the security of the same. The need of for exchanging a lot for our private information and secrete in cyber space. For image security various techniques like cryptography, steganography, visual cryptography, watermarking etc. are present [1].

Cryptography convert secrete data into unreadable form, generally it is called cryptography is a concept to protect network and data transmission over wireless network. Cryptography is the skill of writing in secret code. Modern cryptography exists at the intersection of the mathematics, computer science and electrical engineering. Application of cryptography include ATM cards, computer password, and electronic commerce [3]. Steganography technique is a method of secrete data communication, while the watermarking is used for the copy write protection of the electronic product. In steganography the secrete message is hidden in other than original media such as Text, Image, Video, Audio form [4,5]. Visual cryptography is technique which allow visual information, In the process of visual cryptography a secrete image is encrypted into share which decline to disclose information about the original secrete image. Watermarking is a technique which inserting information. A watermark is a form, image or text that is impressed onto paper, which provide of its correctness. Watermarking is message which is

embedded into digital content. So, these paper survey on the image security or image and image techniques.

II. IMAGE APPLIACATION

The recent practicability of much computer-based technologies has brought multimedia data transformation over the internet. The multimedia data can be included with image or video or audio or graphical objects that contain much important of organizations, governments, hospitals. between the many multimedia, the data image is commonly used for loads of aspects of military, hospital, etc. [1].

III. NECESSITY FOR IMAGE SECURITY

Today's various people utilize the distinctive application to image data transfer. by far most of the people use their image for various customer using the social application. The attacks on these social applications can copy or hack the important data. for better usage of these application, users are using it on their mobile tables, etc. The protection of hacking attacks on these webs or available is plans, there exist distinctive data framework for multimedia data [6]. The transfer of the image over the unsecured network will create following attacks such as:

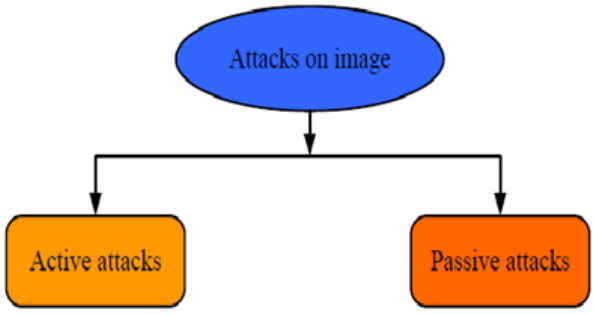

Fig. 1 Attacks on image data

A. Passive attack

This kind of attacks includes observation or monitoring of communication. The goals of passive attack are to gain information that is being transmitted. Passive attacks are very problematic to detect because they do not involve any alternation of data [2,3].

B. Active attack

The second major type of attack is active attack. These attacks involve some modification of the data stream or the creation of the false stream. An active attack attempt to alter system resource or affect their operation [2,3].

IV. TOOLS OF HACKING IMAGE DATA

The history of "Hacking Tools" with its security [1].

C. SN1PER

Sn1per is an automated scanner that can automate the process of collect data for the searching and access testing. In their work sn1per connect such well-known tools similar to: amap, arachni, amap, cisco-torch, dnsenum, golismero, hydra, metasploit-framework, nbtscan, sqlmap, sslscan, theharvester, w3af, whatweb, nitro, wpscan through a penetration test to enumerate and search for vulnerabilities.

1) Feature of SN1PER

- Automatically collects basic recon (i.e. ping, DNS, etc).
- Automatically person forces sub-domains and DNS data.
- Automatically checks for sub-domain hijack.
- Automatically runs under fire NMap script beside open ports.
- Performs high level record of many hosts.
- Automatically integrate among Metasploit Pro, MSFConsole and Zenmap for reporting.
- Create character workspaces to store all search out put [14].

D. JOHN the RIPPER

John the Ripper is commonly used in the activity to detect weak passwords that can put network security at danger, as well as other organizational purposes.

Formerly developed for Unix-derived systems, John the Ripper is available for common platforms. The free and open source (FOSS) version is generally circulated as source code. A commercial version, John the Ripper Pro, is a more available version distributed as native code for a given system password entropy, password blacklist, password strength meter [posted by Margaret rouse]

1) John the Ripper password hacker
2) Lience/price: freeware
3) Version:1.8.0
4) File size:4.3 mb
5) Developer:jhon
6) OS: Windows

E. NMAp

Nmap (Network Mapper) is a free unlock source protection tool used by infosec professionals to handle and check network and OS security for both local and remote hosts. Despite being one of the oldest security tools in reality (launched in 1997), it continues to be actively updated and receives new improvements every year. It's also regarded as one of the most helpful network mappers around, known for being fast and for always deliver thorough results with any security investigation.

F. WIRESHARK

Wireshark is free open-source software that allows you to evaluate network traffic in real time. Wireshark is generally known for its capability to notice security problems in any network, as well as for its effectiveness in solving general networking problems Wireshark supports up to 2000 different network protocols, and is available on all major operating systems including:

1) Linux
2) windows
3) Mac OS X
4) FreeBSD, NetBSD, OpenBSD

V. IMPORTANT METHOD FOR IMAGE SECURITY

A. Cryptography

Cryptography is a method of storing and transmitting data in particular form so that only those for whom it is intended can read and process it the term is most often associated with plaintext message into cipher text. Generally classified into three type [7]:

1) Symmetric key (secrete key)
2) Asymmetric key (public key)
3) Hash key.

1) Symmetric Key:

In symmetric key, a single key is used for both encryption and decryption. Symmetric key schemes are generally divided into block ciphers.

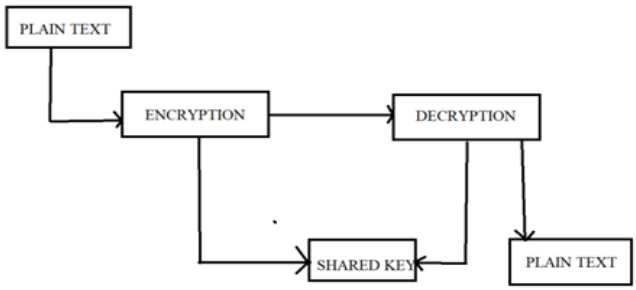

Fig.2 Secrete Key Cryptography

2) Asymmetric key:

Asymmetric key is forms of cryptosystem in which encryption and decryption are perform using the special keys, one is public key and one is private key.

3) Hash key:

Hash key, or secure hash function, is important not only in message authentication but in digital signature [2].

B. Steganography

Steganography is the study of technique for hiding the reality of secondary message in the presence of a

primary message. Steganography is the art of science of hiding the fact that communication is taking place. Send the stegno-message above the insecure control to receiver [15].

Different types of steganography are as shown in figure They are as follow:

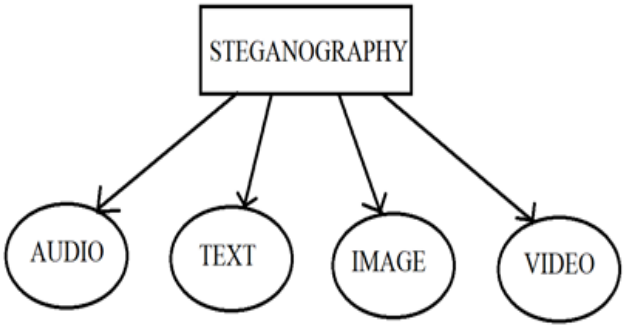

Fig. 3 Type of Steganography

1) Audio steganography

In audio steganography type secrete data can be hidden after any audio media. Generally, two types of audio are used in this type. One audio file performs as cover media while another file is secret message.

2) Text Steganography

In this type the secrete data can be hidden after any text file which can be sent across an unsecure channel. Example: Message to send: Since Yug Can Run, Encoding Text in Natural Surrounding Is Deliberately Effective. Original Message: Since Yug Can Run, Encoding Text In Natural Surrounding Is Deliberately Effective. Secrete Message: SECRETE INSIDE

3) Image Steganography

In this type, hiding the data behind the cover image is referred to as image steganography. Pixel intensities are converted into binary image to hide information in the most redundant bits. After embedding the stegno image is generated this can be transferred above an unsecured channel.

4) Video Steganography

In this type the secrete data can be hidden behind a video file so that a large amount of data can be hidden behind. Video steganography is becoming an important research area in different data hiding technologies, which has become a capable tool because not only the security requirement of secret message transmission is suitable stricter but also video is more special. So, these are very important type of steganography.

C. Watermarking

Digital Watermarking describes methods and technologies that secrete information. The embedding takes place by manipulating the material of the digital data. Watermarking is the addition of invisible and inseparable information into the host data for data protection & reliability. Another type of digital watermarking is known as steganography, in which a message is hidden [8].

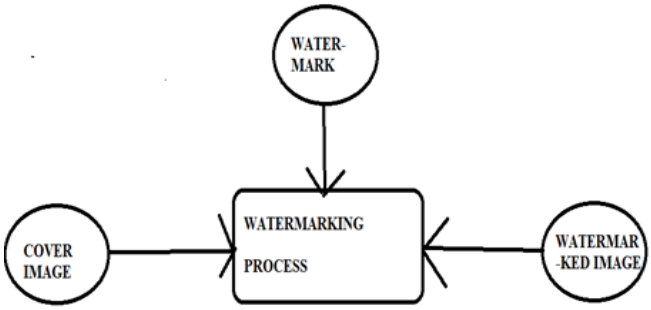

Fig. 4 Watermarking process

Digital watermarks are of four types:

1) Visible
2) Invisible
3) Robust
4) Fragile
1) Visible

A visible watermark typically consists of a clearly visible message or a company logo indicating the ownership of the image. Any deletion o with the logo would break the copyright agreement. Another way is to write the copyright notice and other information into an extra team of lines within the image file. The extra lines can be removed from the image, without damage to the image quality and content, but this again would break the copyright agreement of the image.

2) Invisible

An invisible watermarked image appears like to the original. The existence of a hidden watermark can only be determined using an accurate watermark extraction or detection algorithm. It can be detected by a formal activity only. Such watermarks are used for content and author verification and for detecting unauthorized copier.

3) Robust

Robust watermarking is the watermarking algorithm that can carry on not only such general operations such as compression, adding noise, filtering, A/D or D/A conversion but also such geometric attacks such as rotation, scaling change. It is often used in ownership security.

4) Fragile

Fragile watermarks are known as tamperproof watermarks. Such watermarks are not working by data management. Fragile watermark is a mark which is approachable to a variation. The fragile watermarking scheme should be capable to detect any change in the signal and identify where it has taken place and may be. It serves at proving the accuracy of a document [9].

VI. IMAGE SECURITY TECHNIQUE

There are numerous security techniques are available for the security of digital image. Following table represent the numerous security technique which are found in the literature for the security of digital image [12].

Table various security techniques:

Authors	Suggested Technique(s)	Concluding Remarks
Chen and Lai [1]	Cellular automata using recursive substitution and random sequence to perform confusion diffusion for image security.	The secrete key with variable length, safeguard against cropping and replacement attack.
Al – Husiany [2]	Confusion diffusion performing XOR operation to right rotates pixel bits to encrypt image.	Simpler and strong because of XOR and long key
Azam [3]	Steganography using gray scale substitution boxes using fuzzy logic and phase embedding technique.	Used two random masks in frequency and spatial domain, the cryptosystem is state of the art and suitable for color image .
Pushed et al. [5]	Combined procedure of image encryption and reversible watermarking embedding in frequency domain.	Increases confidentiality and efficiency
Verma and Jain [6]	Image encryption using less complicated technique dual tree complex wavelet transform	The image is too highly secured for transmission.
Garg and Kaur [8]	Hybrid approach using steganography with color illumination-based estimation and encryption with the help of AES.	Encrypted images bits altered with least significant bit which not affect the quality and seems like original
Badshah	Watermarking	Recovers the altered

[10]	technique using lossless compression.	image due to noisy channel or intruder

Table 1 Image security technique

VII. COMPARISION OF METODS FOR IMAGE SECURITY

Table 2

	Steganography	Cryptography	Watermark-ing
Definition	Is the art and science of secreting data.	Is the art science of hiding information.	Is the process of embedding a message on a host signal.
Secrete message	Is unreadable and data is twisted.	Data is hidden and is not twisted.	Is invisible or visible depending on requirements.
Security	No one would be capable to know the message say unless there's a key to code. .	The hidden message is imperceptible.	An unauthorized person cannot detect Riverview or transform the embedded watermark.
Capacity	Differs as different technology usually low hiding capacity.	Capacity is so high, but as message is long it changes to be decrypt.	Capacity depends on the size of hidden data.
Techniques	LSB.	RSA, transposition	DCT.
Input files	At least two	N/A.	One.

VIII. FUTURE SCOPE

In future the study can be supported as followed:

- A test bed can be planned by considering the adversarial element (considering differential attack) and user element control of classified data over the network.
- A cryptographic frame can be designed for simple function of image verification.
- A mathematical operation can be performed such as repetition relative and polynomial mapping for structure the strength in security.
- An evolutionary algorithm can be used to convey the potentiality in cryptographic process.

IX. CONCLUSION

This paper presents the survey over different techniques of image security and literatures of offered research work. Currently image is most generally used communication mode in special areas medical area, research area, business area, military area etc. The important image transmit will take place over the unsecure internet network. Hence Security is the major concern for any scheme to maintain the reliability, privacy and image accuracy. Although cryptography is the effective method but it also face the difficulty in providing the security if the data in the image is more. This paper discussed the Necessity for image security, Encryption performance parameter,

image encryption methods, Cryptography methods and important methods for image security and current work on it. The study analysis of the open research work helps in defining the research gap and providing the future research line for image protection even better.

X. REFERENCES

[1] Peres, Elizabeth M., and John A. court right "Normative image communication media mass interpersonal channels in the new media environment". Human communication research: 485-503

[2] William stalling" network security Essential application and standards {book name}

[3] "Shyam Nandan Kumar" Technique for security of multimedia a using Neutral Network.

[4] PATEL P, PATEL Y Secure and authentic DCT image Steganography through DWT-SVD based digital watermarking with RSA encryption. proc. Of the 5th international conference on communication system and network technologies ,2015(736-739)

[5] LASKAR TA, HEMANCHANDRAN K. Digital image watermarking technique and application. International Journal of Engineering Research and Technology ,2013.

[6] Hill, Douglas W., and James T. Lynn, Adaptive System and method for responding to computer network attacks V.S patent No.6,088,804,11july 2000

[7] Diffie, w. Hekkmon, M (1976). New direction in cryptography. IEEE Transcation on Information theory 22(6) =644-654

[8] Gray L Fridom, trustworthy digital camera restoring credibility to the photographic image, IEEE trans. consum. electron.39(4)(1993) 905-910\

[9] Dr. Rajib Kumar Bhattacharya, introduction to genetic algorithm.

[10] A. E. Ebien, R. Hinterding and ZMichakewicz,"Parameter control in evaluationary algotithm",IEEE transcation on Evaluatory computation :on pp-124-141.

[11] Digital image security: fusion of encryption steganography and watermarkinhg

[12] F. Djebbar, B ayaady, H.K.Abed Meraimx " A view on latest audio steganography techniques", International Conference on Innovations in Information Technology , 2011.

[13] SN1PER – A Detailed Explanation of Most Advanced Automated Information Gathering & Penetration Testing BY Balaji in 16 February 2019

[14] Intelligent Processing: An Approach of Audio Steganography. 2011.IEEE

[15] elprocus .com/artificial-neural-network-ann-and-their-type.