Review of digital data protection using the traditional methods, steganography and cryptography

Chinmaya Dharmadhikari and Rejo Mathew

October 16, 2019

Review of digital data protection using the traditional methods, steganography and cryptography

Chinmaya M Dharmadhikari[1], Rejo Mathew[2]
[1]Department of I.T. Mukesh Patel School of Technology and Management,
NMIMS, Mumbai, India
Chinmaya2903@gmail.com
[2]Department of I.T. Mukesh Patel School of Technology and Management,
NMIMS, Mumbai, India
rejo.mathew@nmims.edu.in

Abstract – The following paper reviews software protection methods using the methods of steganography, cryptography to safeguard the running applications on pc as well as mobile applications. The software applications these days gets most of the work done for professional use as well as other purposes. The major issues faced by the software developer or publisher are of software piracy. All the major software these days are circulated and pirated through the internet. Thus using steganography other techniques the goal is to solve the problem of software piracy. The solutions for protecting software from getting pirated are stated in this paper.

Keywords – Steganography, Data protection, Stego image, Software developer ,JSON, HDD, MAC Address, Database , LSB(least significant bit) , ciphertext ,StegoDB , XOR , Blowfish, Edge detection

1 **Introduction** – The information exchanged over a computer is mainly through network and files stored in computer are in various forms of format such as text, image, sound .The information stored or the software used can be easily copied which is one of its greatest weakness. In today's world due to digitalization ecommerce or banking transaction are processed. To protect this type of data encryption methods are used.

Steganography is defined as the scientific method of hiding information within an image. Data which is protected using steganographic methods is more concealed by encryption methods before applying the steganographic processing to it.

To reduce the piracy issue companies employ different methods such as licensing acts, patents ,cryptographic methods and dongle.

The following paper reviews the software protection framework which uses the cryptography, steganography and the new processes to protect the traditional desktop applications as well as mobile applications.

1.1 Hardware means for protection of the software

Due to the software being connected or accessed through internet software gets exposed to piracy. So, the software protection is carried by the developers who provide a special hardware which has to be connected when the software is being used by the user.

USB/Serial port dongle: The most common hardware protection method available is dongles. For software to work the dongles need to be connected to the software all the time. When the software starts to execute operation the software primarily checks the port in which dongle is present and checks in memory that the encrypted key is present or not. If the key is similar with the registered information then the software is executed. If the key is not similar with the information then the software will throw an error. Using a dongle based system often proves costly as it requires some special types of drivers to make the dongle work. It becomes difficult to implement this method heavy use environment where there is need to install software on many computers.[3]

1.2 Methods of protecting a software with support of hardware

This method implies that, the software use various methods for protection of data using software means which help in authentication of the users connected or using a specific software. These methods generally recognize the device on which the user has connected the software or a designated id is given to a user through which a user can register himself with the software.

1.3 **Software means of protection**

The several methods used for protecting the information is given in this method. The techniques provided through the software means are feasible for the individuals who are sole proprietors of the firms. This methods use techniques of cryptography which converts plain text to cipher text and steganography which is protection of the text inside the image[1]

1.4 **Exposure of the techniques using hardware means ,software means of protection**

i. While considering above techniques protection methods using hardware are not easy to implement as they require some specific features, additional dongles so these techniques are not feasible to use.

ii. The techniques are neither cost effective. These techniques has various vulnerabilities and through those vulnerabilities crackers with the help of hardware methods try to write the backdoor programs and can clone the functionality which bypasses security.

1.5 Multilevel hiding text security technique

i. This technique uses various processes to protect data. Following are the steps in which the given process advances

Step1:The first process is to encrypt the secret message using a blowfish algorithm to generate a key which is used in encryption process with XOR a plain text with key. Blowfish algorithm is a block cipher algorithm which uses symmetric key that encodes 64-bit block

Step2: In second process the hiding positions are determined using the edge detection algorithm to cover a image. The proposed embedding method utilizes Sobel edge detector on every 3 × 3 non-overlapping block of the cover image .Sobel operator is a mutually perpendicular gradient vector field operator

Step3:In this step Bats algorithm is used to cover the image which has been obtained by the edge detection to pick a random hiding position in the image which is obtained by edge detection. Bats algorithm is an optimization algorithm depends on the echolocation behavior of bats when searching for preys.

Step4:The last step is to embed the message using LSB(Least significant bit)

2.1 Applications of the Hardware means for protection of the software

i. CAD/CAM software: Computer aided Design or computer aided manufacturing software are widely used in the industries like oil ,mining. They are costly to develop so use dongle based protection against the piracy

ii. Animation/ 3Dsoftware : These software also cost thousands of dollars to develop so they basically use dongle based protection

iii. Steinberg key: This product protects Steinberg products which protect audio and also the editing solutions . In Steinberg key dongle apart from software protection it also provides another feature in which only the modules purchased or bought by the user are unlocked..

iv. Smart cards: Smart card is the recent development in the hardware based protection to use . In smart card protection a card reader is attached to the system and the inserted card is read and the access is provided to the software [3]

2.2 Protection of software with support of hardware

i. Serial Numbers: Serial numbers is the simplest method used in software protection . A serial number is created with help of c algorithm to the specified user who has a licensed version of software. Further developments to these methods were brought by the game developers which ensured that in a cd drive a cd is present when the game is running. Further advancement included the use of digital signature into disc produced at the time of manufactures . When the software is running they will check the presence of the cd and the copy protection digital signature on the disc. A special hardware is required to manufacture disc with digital signature

ii CD Based protection: The copying of music from CD's and DVD's is the most common thing in which the ripping software is used to convert the audio cd's to mp3 music. To prevent the ripping several studios introduced the software which monitors and executes when DVD/cd is inserted into the computer. The software monitors if any ripping software is being run or not and if its finds it disables the access to the drive or stops the software from doing this

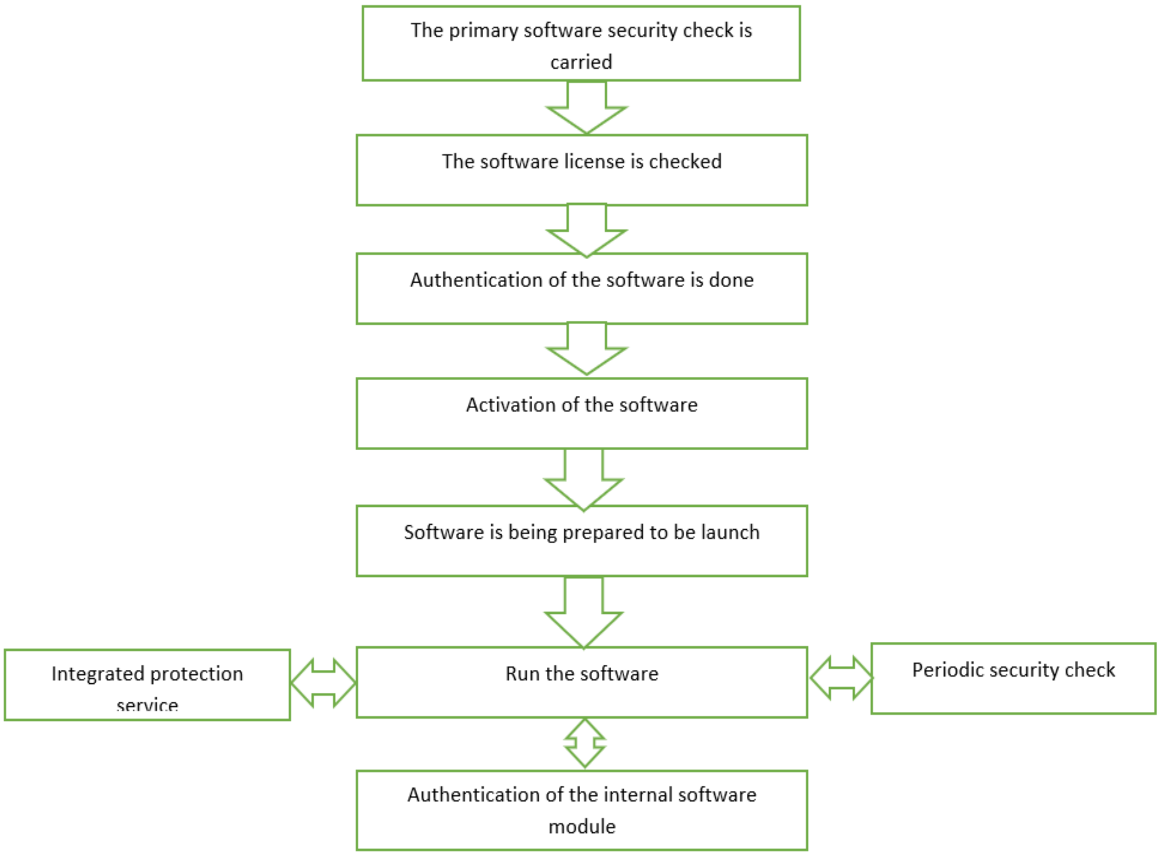
2.3 Applications used for the software means of protection

i. Cryptography: Cryptography is the scientific method to use the secure convention . The conversion of plaintext to ciphertext to prevent the unauthorized access to the message /information. The various algorithms developed to protect the data are DES(Data encryption standard),TDES (Triple data encryption standard),RSA,AES(Advanced encryption standard). AES is employed by the government of USA

ii Steganography: The further version of cryptography is steganography. The protection of information inside the image is done in the steganography for e.g LSB,RGB,PVD etc .Water marking and visual cryptography are some of the techniques used for protection of the data

- **ARCITECTURE OF SOFTWARE PRTECTION:**

The following diagram represents that what are the steps in which a software authenticates a user and checks the software license and authenticates the hardware. After reading the license and hardware the activation of the software takes place and in the final step the software gets prepare to launch . While execution of software takes place the integrated software execution, authenticates the internal modules and periodical security check takes place after each function in the software is been executed [3]


The primary software security check is carried
The software license is checked
Authentication of the software is done
Activation of the software
Software is being prepared to be launch
Integrated protection service
Run the software
Periodic security check
Authentication of the internal software module

Architecture of software protection framework

2.4 **StegoDB model**

The following technique combines the advantages and disadvantages of the existing framework and reviews a new framework which contains cryptography, steganography and hardware features . Designing of this method is such that execution is easy and breaching the security is difficult for the crackers. The technique gets implemented using the following steps
A. Software protection framework: The proposed technique consists of two parts the authentication algorithm and protection algorithm.[4]
Step1:Authentication algorithm carries out the registration process
Step2:Creation of stego token and attaching it to software for protectionStep3:Software execution is the final step where validation algorithm validate the authenticity

Authentication Algorithm:

Step 1: The user information, Hdd serial number or MAC address should be fetched to determine a distinctive i.d which can be used to verify the distinctive properties of the device[4]
HDD serial number can be found by the following commands
1. win32_DiskDrive API should be cited
2.Select the serial number
WIN32_DiskDrive API is provided by windows to extract the serial number
Step2:The serial number is encrypted using the AES encryption standards and stored in read only file
Step 3: The file is sent to licensed server of the software which is present at the software providers end. The

server will provide the HTTP API’s. The server than provide the HTTP API’s for receiving the file . SFTP file transfer protocol can also be used to transfer the file
Step4:Fetching of user mail id along with information should be done. Step 5: The authenticated user information is saved in the licensed server

ii **Protection Algorithm**:

Step1 :Using the authentication algorithm creation of user authentication information is done
Step2: Provide the user i.d information from the file stored
Step3: The SteganoDB package should be applied steganoDB structure, [2]

```
{ "First Name": "ABC",
"Last Name": "ABC",
"Email":"ABC.ABC@tcp.com",
"Address Line1":"125#sector 78",
"Address Line2":"M-Nagar",
"Address Line3":"Mumbai-30",
"Phone":"989"
"Key":"UdGkX1/IiYCbur74I5oNTBL/nBa MPfgg+s="
}
```

SteganoDB is a database structure which is used to embed the data in images that can be read or retrieved efficiently. SteganoDB is created using the JSON structure associated with steganography to create the SteganoDB which is unique. Username, email, addresses can be stored in this steganoDB and can be extracted with the modern programming language[2]
Step4: The encrypted data is embedded in the given image which the pixel pattern based steganography algorithm. Due to the use of pixel pattern cryptography the quality of image does not degrade and image which is covered will not appear to be different and would be free from attack . Encryption and steganography are two techniques used to protect the information[8]
Step5: The encoded image file is saved at the receivers end and as the stegano key is generated it is sent back to the software running on the desktop. This can be accomplished using the secured protocols like http(https) or ftp(sftp)[9]
Step6:The protected software checks the encoded key for each of the execution
Step7:Extraction of key from the stego image.
The algorithm for the following is as:

```
To extract key from the server, the following methods should be followed
{
The characters in image metadata should be selected
{
The pixels in the image should be noted
}
The mod bits from the pixel positions should be found out[7]
The given mod bits should be decrypted     }
```

After execution the algorithm will fetch following results primarily serial number would be extracted and the reverse AES process would decrypt the following
Step 8: If the key does not match or if someone is trying to breach the security of software by installing it on another PC where the installed software is and the key then comparison of the steganography with the hardware properties of the PC is done which will fail and the software will indeed remain protected[7]
Step9: Regular self-checks of the software can be done by placing the key properties in .crc file. As the software executes it checks the properties with the stegano file and if it is false execution of software is stopped.

iii Data base Algorithm: Secure transfer of database or file from device to device is done using these algorithms. The process can be used to protect the database or sending files from device to device using the proposed steganography algorithm and steganoDB
Step1:The image file on which the text should be embedded should be selected Step2:Choose a secure password for protection of database Step3: The software will request for a one time key from the receiver side. From the receiver side the software will detect the hardware property of the device like the hdd serial number etc. This will be the unique id for identification to software.

```
{ "First Name”: "ABC",
"Last Name": "ABC",
"Email": "ABC@tcpcom",
"Address Line1":"124#Lane 15",
"Address Line2":"M-Nagar",
"Address Line3":"XYZ-60",
"Phone":"989"
"Key":"U2FsdGV19L7/IiBYbur74I5oNTBL/nBa MPfgg+s="
}
```

Step4: The text is converted into JSON structure

Step5: Apply stegano DB to the password and the hardware property of the device [2]

Step6: The steganography data embedded algorithm is applied and choose the file to protect

Step7:Send the stegano image file via file transfer protocols

Step8: Receiver will receive the file and save it

Step9: The hdd number is checked and it uses a password to decode.WIN32_DiskDrive API is used to retrieve serial number from hard disk

Step10: using the retrieving algorithm decoding of the image is done and the separation of text from image is carried

Step11:The text is read in JSON format and stored in.txt file

This method helps in protection of the databases or text files

iv Mobile Data protection

The algorithm can also be further implemented in the mobile applications. The framework remains the same except instead of HDD serial numbers the mobile will use the IMEI number. The access of the app can also be made limited to a certain region using GPS. The following information can be hidden using steganography and thus protected [10]

2.5 Multilevel hiding text security technique

The key generation and the embedded as well as the extracted algorithms are discussed in this technique

i.**Key generation and encryption algorithm**

In this algorithm as a input there is requirement of color image and plaintext and output obtained is the key so the following steps have to be followed as loading of BMP color image and key generation should be done using the blowfish algorithm and after that conversion of input image to binary image should be done and them the image should be divided into 64-bitsblock as plaintext. Load the plaintext in different size and then divide the text into blocks of same size as the key. Apply XOR between the key generation and plaintext with different size to obtain ciphertext[4]

ii.Embeded Algorithm

In this algorithm color cover image and ciphertext is taken as input and the output obtained is a stego image. In first step load the BMP color image and then apply edge detection algorithm using the sobel filter. Apply bat algorithm on the output which is obtained after edge detection to choose random position. Ciphertext is embedded using LSB technique to generate steganography image[4]

iii.Extracted Algorithm

This algorithm uses input as Stego image and gives output as plaintext . In this edge detection is applied on the stego image using sobel filter and then apply bat algorithm on stego image to select random positions and extraction of ciphertext is done using LSB and apply XOR on ciphertext to get the plaintext [4]

II Analysis/Review

Comparison table

	Hardware means of protection for software	Methods of protection using Software with the help of hardware	Software means of protection	Stego DB technique	Multilevel hiding text security technique
Functionality	user connects the dongle for the software to work	Generation of serial numbers, digital signatures required for CD etc	Steganography is used with cryptography to increase the security of data transfer	Cryptography , steganography ,Authentication algorithm, Protection algorithm	blowfish algorithm, bats algorithm and edge detection algorithm
Implementation areas	CAD/CAM software, Animation software , Steinsberg key	CD based protection, DRM services(Digital Rights management)	DES(Data encryption standards) , AES(advanced encryption standards) implemented using cryptography,	used in authentication mechanisms as well as software protection mechanisms which also include database protection , security checks etc	This technique is used in sending messages from different networks and the data is converted into ciphertext and then covered in a stego image
Security level	The data could be breached if the hardware component is damaged. Thus the security level is low	The data in this method is not secure as it is easy for hackers to make a copy of software	Better security level but implementing various algorithms like DES,TDES is difficult for organization	Due to dual layered protection and acquiring the physical address of hardware component on which software is installed it is difficult for crackers to exploit the software	It is well structured algorithm and the ciphertext when inserted in a stego image gives a good security level
Vulnerabilities	If crackers find presence of a hardware device, then using backdoor program to clone the functionality of the hardware	The CD protection can be manipulated using the cloning	Side channel attacks are threats to these protection methods	No potential third party attacks unless user does not disclose the id and password, a secure method to protect data	colluding attack on the blowfish algorithm can result in combining multiple copies of data and in edge detection algorithm replacement of linear combinations of data will be done
complexity	less complexity	This method has moderate complexity but security cannot be trusted	This method has high level of complexity and cumbersome to maintain	Highly complexed and secured	Highly complex and secure

III Conclusion and Future Work

The paper reviewed has discussed various techniques which include digital data protection methods or the methods which avoid the piracy of data. Primarily the paper reviews all the traditional methods used which include the hardware methods, software methods. The following traditional methods gets vulnerable to threats and piracy so a new technique is reviewed using steganography and cryptography .The technique uses pixel pattern based steganography algorithm which combines it with encryption and unique hardware properties. The algorithm becomes hard for the crackers to detect as it uses same pixel patterns and strong encryption algorithm like AES which provides high level secured protection. The given techniques does not need any external hardware like the traditional methods which use dongles which makes them exposable to the threat . Due to layered protection given in the framework it becomes extremely hard for the hackers to crack the software

The process of hiding information in text security technique is followed by various steps. The secret message primarily is encrypted by blowfish algorithm which generate the secret key and XOR it with the plaintext and then the hiding position is selected by edge detection and then the bats algorithm and LSB is to embed the data in image. These parameters give high performance in data transmission and improve the quality of the method

References (IEEE format)

[1] R. Rejani, D. Murugan and Deepu V. Krishnan:Novel Software Protection Framework Using Steganography, Cryptography, Uniqueness of Hardware and Self-Checks In:International Journal of Advanced Information Science and Technology, Vol. 25, No. 25, pp. 32-40, 2014.

[2] R. Rejani, D.Murugan and Deepu V. Krishnan:STEGANODB-A Secure Database using Steganography.In: ICTACT Journal on Communication Technology, Vol. 4, No. 3, pp. 785-789, 2013.

[3] Bertrand Anckaert, Bjorn De Sutter and Koen De Bosschere:Software Piracy Prevention through Diversity In: Proceedings of the 4th ACM workshop on Digital rights management, pp. 63-71, 2004.

[4] Noor Hasan Hassoon , Rajaa Ahmed Ali , Hazim Noman Abed , Adel Abdul-Jabbar Alkhazraji:Multilevel hiding text security using hybrid technique steganography and cryptography In:International Journal of Engineering & Technology, 7 – 4-2018 ,3674-3677

[5] S. Phad Vitthal, S. Bhosale Rajkumar and R. Panhalkar Archana:A Novel Security Scheme for Secret Data using Cryptography and Steganography In: International Journal Computer Network and Information Security, Vol. 4, No. 2, pp. 36-42, 2012.

[6] Shamim Ahmed Laskar and Kattamanchi Hemachandra:Secure Data Transmission Using Steganography and Encryption Technique In: International Journal on Cryptography and Information Security, Vol. 2, No. 3, pp. 161-172, 2012.

[7] Minati Mishra, Priyadarsini Mishra and M.C. Adhikary:Digital Image Data Hiding Techniques: A Comparative Study ANSVESA, Vol. 7, No. 2, pp. 105-115, 2012.

[8] R. Rejani, D. Murugan and Deepu V. Krishnan:Pixel Pattern Based Steganography on Images In: ICTACT Journal on Image and Video Processing, Vol. 5, No. 3, pp. 991-997, 2015.

[9] R. Rejani, D. Murugan and Deepu V. Krishnan:Comparative Study of Spatial Domain Image Steganography Techniques In:International Journal Advanced Networking and Applications, Vol. 7, No. 2, pp. 2650-2657, 2015.

[10] Richa Raja Gautam and Rakesh Kumar Khare:Real Time Image Security for Mobile Communication Using Image Steganography In: International Journal of Engineering Research & Technology, Vol. 1, No. 8, pp. 1-5, 2012.

[11] Sharmishta Desai, Sanaa Amreliwala and Vineet Kumar:Enhancing Security in Mobile Communication using a Unique Approach in Steganography In: International Journal of Computer Science and Mobile Computing, Vol. 3, No. 4, pp. 433-439, 2014.

[12] Vinay Kumar Pant, Mr. Anshuman Saurabh:Cloud Security Issues, Challenges And Their Optimal Solutions In:International Journal of Engineering Research & Management Technology, ISSN: 2348-4039, Volume 2, Issue-3, May- 2015.