International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Information Security Management of Confidential Corporate laptop Data using Steganography

Anu Binny[1], R.N Duche[2] , Dr. K Maddulety[3]

[1]Research Scholar, Mumbai, (India)

[2]Lokmanya Tilak College of Engineering Mumbai.(India)

National Institute of Industrial Engineering, Mumbai, (India)

ABSTRACT

Today there is a paradigm shift in the way we look at securing assets. In a time where knowledge is the most important asset there is need to look at securing these assets in a different way. Based on the review literature it has been observed that laptop stolen/lost can be possible threat to leakage of confidential data. Most of the stolen laptops are never recovered. Though data backups are available on company server and user can resume office work immediately, a major threat still exists. The documents are available on the stolen laptops and can be easily retrieved and leaked. This research makes a novel contribution by suggesting that a more complete and comprehensive approach to information security is required. We recommend that users play an effective role by hiding confidential data by using the suggested technique. An approach involving the knowledge force by sharing the ownership of managing the security of important information with the knowledge owners' has been explored and illustrated in this paper. Cryptographic steganography has been used as the technology for hiding the confidential data and a case study also has been taken up to understand the probable use of this approach. It is proposed that if owners of data are able to hide valuable information by using Crypto-steganography it can have a major effect on security management. This research also unlocks up potential opportunities for further research.

Keywords-Security management, lost laptops, Information security management, encryption, Crypto-steganography.

I. INTRODUCTION

Steganography is an idea to hide information by hiding the presence of the message. The original files which is used to carry the data is called to as "cover " If the original file is image it is called cover image. Audio or video signal is also used to hide data. The original file plus the secret contents is the "stego-medium". A "stego-key" is employed for inclusion of message to ensure it is unnoticeable and/or thwarts the recovery of the inserted data. The cryptography technique secure the content of data, steganography hides the data so that the intruder cannot see/detect the message. Lot of literature providing a good read to help understand how steganography originated and came to be widely used can be found [1–2].

Stego approaches are the algorithms which conceal the presence of the message itself and easily go unnoticed. To transmit message secretly it is implanted into a stego medium. Location identification of embedded data makes difficult in this case. In case where steganography and cryptography are combined, even if steganography algorithm unsuccessful, the data cannot be extracted since a crypto technique is utilized at the same time. The

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

extraction process of message from stego medium is known as steganalysis. The intention of steganalysis is to find the data and deciding the information is present or not and if possible, extract the hidden information.

Usually security management is looked upon as a problem of the IT department. We are in the era where knowledge, innovativeness is important to sustainability of business. Knowledge is an invaluable asset and if it falls in the hands of the competitor it can provide competitive edge or even a lead to change in their strategic decisions. Additionally companies are becoming more customers oriented and with customer service moving to customer delight there is a need to share confidential data with employers. This confidential data is stored in user laptops. Hence while managing security and understanding risks it is important to change the way we look at security management. It cannot be a centralized approach with the onus of managing it lying in the hands of security or IT department. It has to have a much more decentralized approach and include the owners of the confidential data. Security policy must make it mandatory for the owners to take care of this by using proper access control rights and keeping it in secure servers. But still there is an unaddressed area i.e Loss of confidential data when laptops are stolen/lost. Now this data still resides in the lost laptop in the form of documents or in mails as attachments etc. By ensuring we have backup policy, in case of loss of laptop, users may resume the work immediately by recovering all their information from the servers on a new laptop. But the risk still exists. What about the confidential data that is lost along with the lost laptop? Encryption can be an approach but has its own limitations. Also as users are involved the security management, the tool should be simple to use, should be ambiguous and camouflage it existence and should not cost more than the cost of confidential data residing on the laptop. With these requirements, steganography seems to be a good option. In today's world it is not uncommon to have a large repository of pictures saved on every laptop. So in this paper for security management, the use of images to encrypt confidential data is being studied. To add an extra layer of security, instead of simple steganography, crypto-steganography is used. From the perspective of improving the effectiveness of security management it is proposed that each individual owner should be made aware of the value of the confidential knowledge and the risk associated with loss of laptops. Once awareness is created each owner can be proactive in safeguarding the confidential data stored in his own laptop. So this is the first study of this kind and thus makes a significant contribution on Data loss prevention controls .Moreover we have considered a test case and provided empirical results of applying Crypto-steganography to a business context.

II. SECURITY IMPLICATION DUE TO LOSS OF LAPTOPS

Protection and security of confidential asset are prerequisite to ensure business continuity and efficiency and to circumvent breaches of statutory, regulatory or contractual obligations. Hence security management has taken up prime prominence in all strategic decisions. Security management is the identification of an organization's assets (including information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets. Also the issue of information security is increasingly important for many corporate leaders and individuals who hold confidential data.

Information security is defined as the preservation of Confidentiality: protecting information from unauthorized access and disclosure, Integrity: safeguarding the authenticity, Accuracy and Completeness of information and

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

processing methods; and Availability: ensuring that information and associated services are available to authorized users when required.

Over the last few years, with the advent of computerization and internet explosion, companies across the globe have witnessed their critical data being lost/stolen or leaked. This data loss for example Sale of customer account details or Intellectual property (IP) has caused significant damage to brand/reputation. IP which is defined as the formulas, prototypes, copyrights and customer lists maintained by a company, can be very invaluable. With more and more companies employing the Bring your own device (BYOD) policy, the knowledge sharing and, accessibility, panorama of storing of data is no longer under the boundaries of corporate storage. With customer expecting service 24X7, and the maximum expected TAT of 24 hours, customer facing employees at every grade must be have access to information they need wherever they are working. Now these advantages come with a disadvantage that they are also highly susceptible to theft. The theft of business laptops and the loss of the confidential and propriety information residing on them can occur when they are in the office or in transit. This leak could unintentional as is in the case of loss of laptop or when a user sends sensitive data through unencrypted emails and instant messages.

The findings of a survey done by the Ponemon Institute for employees with more than 7 years of domain-specific experience provide explanations to the given question i.e- why employees' laptops are at a threat.[1]

Of the stolen laptops surveyed, almost half of them had confidential data on them. All of the laptops contain some sensitive information, but the worth of this data may vary. The worth of the laptops containing sensitive data was estimated to be about $37,00.

Only 30% of the stolen laptops had disk encryption, 29% had any type of backup, and only 10% had any other form of protection. Study shows that more than 60 % of users who carry sensitive data believe that it is the IT department responsibility to take care of their assets and have not taken any initiatives personally to protect it on their own

Many organizations agree that a single person or team cannot be responsible for security management of laptops. While most of the respondents accept that responsibility should be with the business teams or with individuals. Most respondents are aware of an episode in their organization wherein there was a risk of losing confidential data in case of theft/loss.

Studies on security have made it clear that by securing organizations with technology based infrastructure alone cannot lead to a robust security management. The problem compounds when confidential data is stored on laptops and is a requirement for performing their job role. For example, the design team may save its product designs or the HR may store the details of the employee including medical history or data (HIV status), salary details etc. on the laptop, the business team may keep a proposal or RFP document, the operations team may have the work instruction manual or any project specific information. If not available to the user may result in delays and customer escalations.

III. LITERATURE SURVEY

Like other business strategies IT security management issues, strategies should be deliberated in senior management review meetings (2). In the research paper studied, the business necessity of cyber security is it is debated. Present research is more concerned with user's role in information security. The earlier tendency of holding the Information technology department employees, responsible for information security has undergone a

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

sea change. Individual user is believed to be having equal ownership and responsible for information security. It is concluded that it is not just an information technology concern. (3) It argues that a more holistic approach to information security is needed . Rigorous studies of different practices of management focusing on IT security have being done. An approach that links the importance of linking all activities and establishing their relationship with the individual user is not explored and brought together. If partially done the approaches are only theoretical. There are suggestions to empower managers to ensure information security is not breached (4). But a clear way how individuals can play a vital role is still not explored.

In the paper(5) The Challenges of Security Management it is explained that " Information Security management is not a technical issue(6)(7) but is a business or organizational problem that must be defined and solved from the perspective of the organization's business drivers keeping the overall strategy in mind. In the past the approach majorly focused on providing technological solutions to take care of information security management issue. Some studies (8) (9)(10) have explored the point of employees' adherence to information security policies. They have advocated it is in the background of management context that information security issues should be deliberated.

Using backups, encryption techniques are methods which are presently used and are centrally controlled by the security department. But as explained earlier in this paper, security measures involving the owner of the confidential data would be a better approach. For example application locks, locks for hard drive etc. can be considered. But it again poses challenges like storing of passwords, remembering multiple passwords, losing passwords saved on notepads etc. and also how secure is the password can be a debatable question. Very often before the completion of the task these confidential data are reviewed by multiple stake holders and hence stored in their respective laptops.

Steganography is the art of disguising the presence of message within innocent image/Audio or video files. Cryptographic techniques encrypt messages. (11). the aim of the two approaches are different, very often the two technologies seem to converge. Steganography camouflages a message to hide its existence. Even though the objective of both methods is to provide security, combining cryptography and steganography provides additional security. A number of techniques are available It provides data protection during storage and also during collaboration through mails

Crypto-steganography is a technique combining both these approaches. Data encryption is done which is followed by embedding the secret message in an image or any other media .It uses a stego key. In our research we have taken image as the cover image. This approach improves the security of the secret data by making it more robust. As shown in the figure below it also increasing the capacity and security offered Uses for Steganography

Steganography can be used for both legal and illicit purposes. In the scope of legitimacy it means ensuring confidentiality, copyright protection, protection against theft, unauthorized viewing etc. It has also been found useful where there is a need to give information like passwords over an email. It has been widely used for adding a digital watermark to images by embedding metadata to pictures and saving it online for dissemination In case of plagiarism, information about the owner tagged to the image can be used to prove the ownership of intellectual property rights. It can also be used for peer-to-peer private communications.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Steganography is a notion commonly modeled by"problem of prisoner". Fig. 1 depicts the overall structure of the steganography system. The various steps of inserting the data is represented in a graphical manner below in figure 1.1:

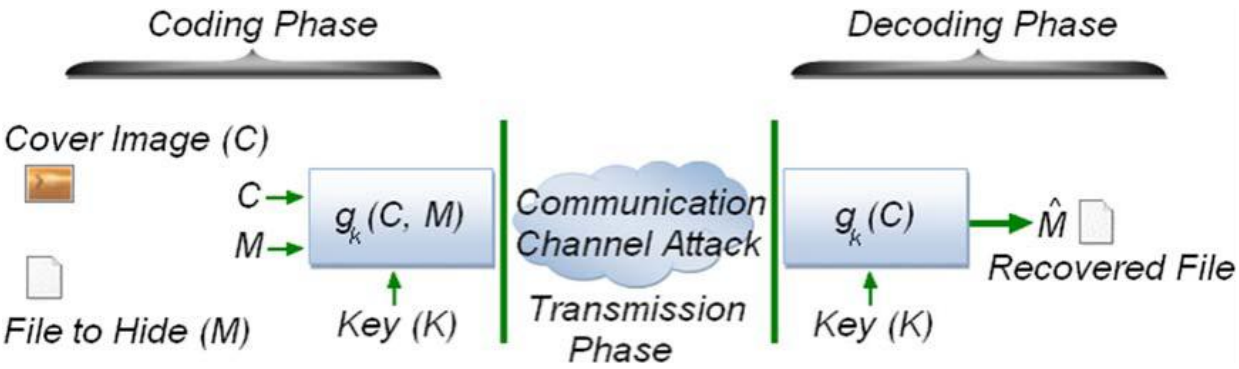

Fig..1 Communication – View of data insertion process flow

Let

C: cover medium i.e. image A

C´: be the stego image.

K: optional key and

M: message to be communicated.

Em: process of embedding and

Ex: process of extraction.

Image is the common file format to insert the secret data i.e. Cover Image

Steganography classification

Information can be hidden inside a cover object using different techniques. As a cover object, we can select image, audio or video file. Depending on the type of the cover, appropriate technique is followed in order to obtain security while embedding the secret data.

Steganography algorithms can be developed by using all the file types, but more suitable formats are those with a level of redundancy. Repeated patterns in the carrier medium will have the higher redundancy. These repeated (redundant) pixels can be exploited for the data insertion process without any noticeable changes that can be detected easily by the attacker. There are many techniques, but a few have been given below Digital image and audio carrier medium fulfill this requirement. Fig. 1.2 shows the various important types of mediums utilized for steganography. Steganography can be divided into five types:

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

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

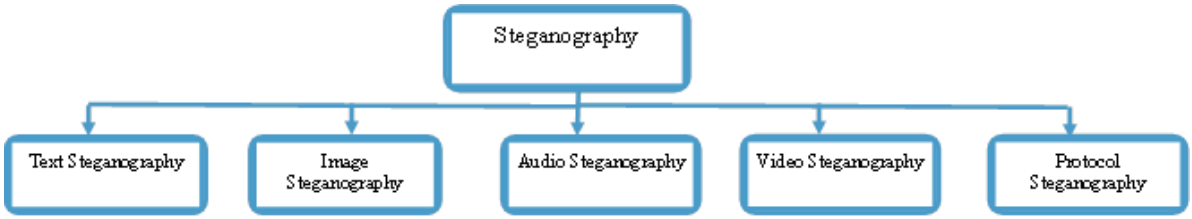

Fig. 2 Classification of steganography

1. Text steganography: Text data hiding is one of the most principal approaches of steganography. In this method, every nth letter of a word has a hidden text or data. Hiding data in text is not popular since the text medium has a very less degree of redundancy.
2. Image steganography: This is a very popular choice of cover medium by various steganography researcher due to the large amount of redundancy. In this technique, message is inserted in an image using an embedding algorithm and by using the secret key. The resulting stego image is sent to the receiver. The secret message is extracted at the destination using the same key.
3. Audio steganography: This approach is moderately employed by various researchers and works by exploiting the human audio hearing capabilities. If two different sounds with different loudness are present then the sound that is louder between the two will be more audible to the listener. This knowledge enabled researchers to choose this area for hiding the data.
4. Video steganography: Video is another popular and widely used cover object for embedding the data. Secret data is embedded using various algorithms.
5. Protocol steganography: The term protocol steganography is embedding information within network protocols such as TCP/IP. Information is hidden in the header of a TCP/IP packet in some fields that can be either optional or are never used.

Spatial Domain Image steganography

The various methods used for image steganography are broadly categorized as “spatial domain” and “transform domain techniques”. Direct embedding of secret message in the pixel value comes under the umbrella of Spatial Domain techniques .Another technique is the transform domain, where instead of directly embedding in the pixel value, using transforms like the image is converted into frequency domain. Later embedding is done in coefficients of transforms. The transforms that are most widely used DCT, DWT, Dual tree DWT, Hadamard transform, Ridge let transform, Curve let transform etc.

It’s a two-step process:

1. **Creation: Combine the message and the cover a stego image is created**
2. **Extraction: message image is separated from the stego image at the receiver. The stego image is created using different algorithms or methods. In crypto steganography secret key is used along with an algorithm to create a stego image. At the receiver end, the message is extracted using decoding algorithm along with the secrete key**

2.1 Applications of image steganography

Image steganography applications in health care

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Telemedicine combines Medical Information System with Information Technology that includes use of computers to receive, store, and distribute medical information over long distances. Also some information like HIV status of a patient is required to be kept secret.

With growing videoconferencing large experts come together collaborate and perform operations. As image is used for diagnosis purpose, even a slight damage to image during alteration methods can result in wrong verdict, incorrect medication and even death. Hence, healthcare industry is also gearing up to use steganography but with high expectations of quality, highly secure, strict authentication.

Criminal photograph authentication and transmission

Most of the crime investigations are based on database submitted to crime branches from remote locations via Internet or mobile phones. When some unwanted crime happens, the criminal(s) photograph is constructed according to preliminary information collected from eyewitnesses where actual incident happens. This sensitive criminal image data needs to be transmitted across network through the Internet or mobile phone. Transmission of such image data demands high and guaranteed security.

Digital copyright protection system based on mobile agent

The advent of digital media and analog/digital conversion technologies, especially those that are usable on mass-market general-purpose personal computers, has vastly increased the concerns of copyright-dependent individuals and organizations, especially within the music and movie industries, because these individuals and organizations are partly or wholly dependent on the revenue generated from such works.

Mobile agent technology and digital watermark technology compensate each other and play a very important role in the industrial applications. The integration of the mobile agent technology and watermark technology has been intensively investigated in recent years.

Health and car insurance companies

Health and car insurance companies use image to store the scanned copies of the medical images of their clients which are stored on the company server or cloud. It is a mandate that this information is stored databases. As it is to be used as evidence or referral during claim resolution, protecting it by using steganography technique is essential.

2.2 Advantages of steganography:

1. It camouflages the existence of message.
2. Steganography can be used to maintain the confidentiality.
3. It can be used to protect if hacked or stolen.
4. Also if used in a secure channel, it can be used to share personal information like Health status (HIV), banking information etc. in corporate environment
5. Audio-video synchronization and TV broadcasting

2.3 Limitations of steganography:

1. Steganography hides a message but the existence of the message can be identified and hidden message can be extracted by various attacks. So, cryptography can be combined with steganography as an additional layer of security.
2. Capacity of hiding is strongly dictated by type and size of the cover medium.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

IV. BUSSINESS CONTEXT

There are various applications that can be considered for this approach. We have used a highly competitive environment industry i.e. the Airline industry. To expand their networks, Airlines are looking out for opportunities that do not ask for making large investment. Hence partnership agreements with other airlines are seen playing a significant role to increase footprint and increasing the customer base .This has led seeing good SPA (Special prorate agreement) as an opportunity for sustaining and increasing business growth.

Importance of this agreement

It has been argued by the industry leaders that SPA can produce 3% and 5% revenue gains for airline by changing strategy to focus on improving revenue and achieving operational efficiency. A well designed SPA enable an airline to offer additional markets and destinations at competitive fares to the market, enabled by acceptable proration cost.

The agreement helps to serve more customers by using the Hub and Spoke model. It also helps in to reduce the overall cost by improving the fleet management and reducing the time. Also by using a planned approach towards fleet management and crew management it is able to improve the operational efficiency. So the carrier can become more competitive with better fares and inventory availability.

Once these agreements are signed it is referred to by many teams and interdepartmental. A focused group discussion confirmed that this agreement is found in the laptops of team members from the SPA department, Revenue accounting team, the commercial team, the Bill team, sales team etc. These agreements often involve revenue risks if it comes in the hands of wrong people .SPA is highly confidential as it gives an information about the processes and strategy, the contract terms, and can provide spying competitors a negotiation edge over pricing and revenue management functions. It can also be used to identify potential partnership opportunities that can be used for selfish gains like expand their own global reach. If put to wrong use, it is also possible that information specific to SPAs can be misused for creating opportunities for the competitors and providing easy inputs to better power led negotiations.

V. PROPOSED ALGORITHM

Application of Crypto-steganography for security management of an SPA agreement:

As the agreement is confidential data and is saved in the laptop during the entire review process. It is also required to refer the documents for decisions. The typical life span of the document is one year. To manage the risk of losing the confidential SPA in case the laptop is stolen/loss the proposed method can be used. Additionally the stego image can also be used for mailing across the teams or to be placed on goggle drive (very often done to facilitate collaboration)

Fig. 3 shows the generalized block diagram of the proposed Steganography algorithm. Detailed description of the schematic is presented in this section.

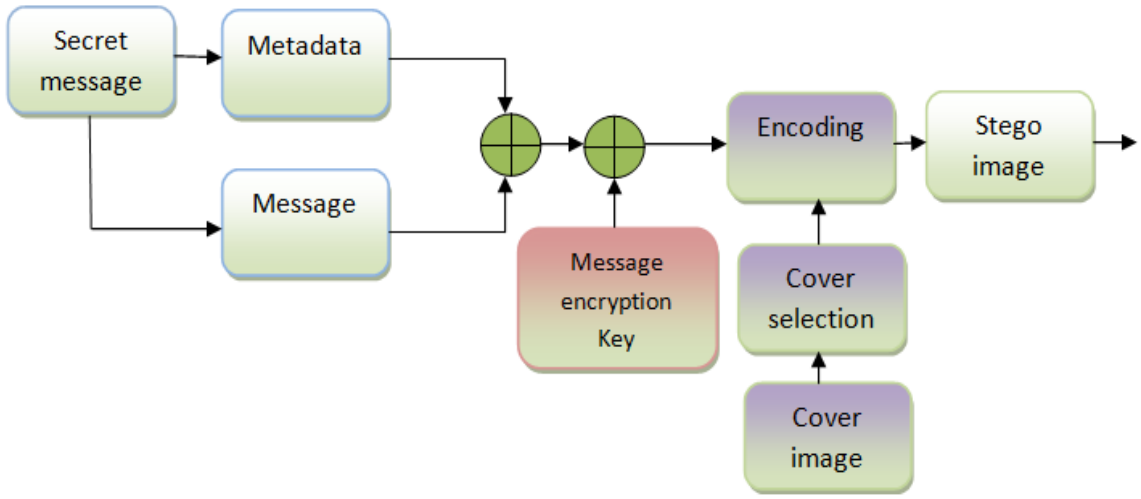

Fig. 3: Generalized block schematic of data embedding algorithm

The main objective of Steganography is to embed the information into the carrier in an imperceptible way to hide the secret data.

In the embedding process, a random key is applied to randomize the input host image. Next, the secret information bits are embedded into bits (LSB) of the pixels. At the receiver end and the transmitter end, the random-key generated using a pseudo-random number is shared. The steps are briefly explained

Step 1: Reading and conversion of the characters from input text file (array of 8-bit integer.)

Step 2: The input color image is chosen in RGB format.

Step 3: Reading of the MSB of the pixel and initialization of the random key.

Step 4: The stego-key is generated

Step 5: XORed with text file of secret text.

Step 6: Replacing of LSB with the bits of the secret text

Step 6: Saving of the stego image

Extraction algorithm:

The random key is required during the extraction process. Procedure can be given as follows:

Step 1: Reading of the stego image.

Step 2: Initiation of the extraction process based on the random key

Step 3: Recovery of the ASCII value of each character.

Step 8: These ASCII values is X-OR ed with shared stego-key which gives the secret message

VI.EXPERIMENTAL RESULTS

This section presents the experimental result of the proposed method. The algorithm is evaluated using color images of size 512 X 512 [USC-SIPI from USC-SIPI image database. All the simulations were carried out using MATLAB 2012a with Core i-3 Processor, 2 GB RAM and Windows 7 operating system. Sample test images

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

from the database and corresponding stego images are shown in figure 3

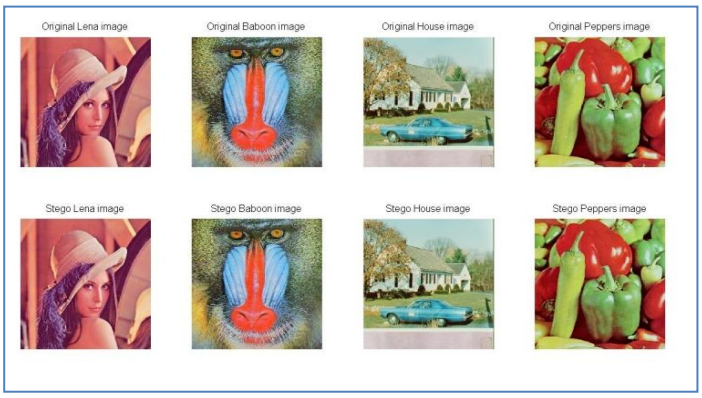

Fig. 4: Original test images and corresponding stego images

First row shows original images and second row shows stego images.

The proposed algorithm hides effectively the secret information bits with minimum visual distortion into the cover image and extracts it efficiently at the decoder side. The resulting stego image has good visual quality. The input message text is shown below

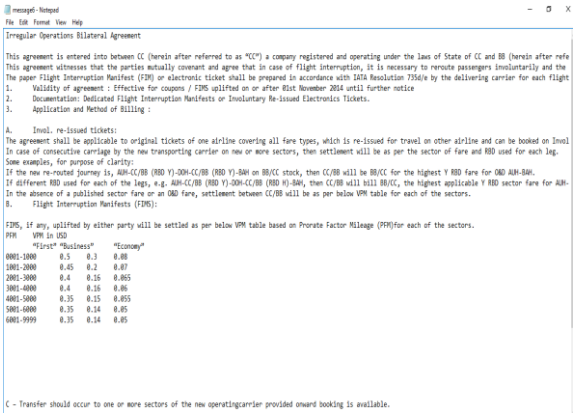

Fig. 5: Secret text decrypted at the Input

The output text post the application of the crypto-stegonagraphic tool is as shown below.

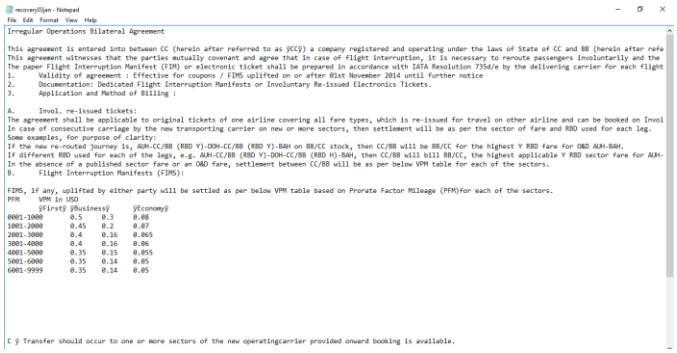

Fig. 6: Secret text decrypted at the Output

Thus this SPA document can be saved in an innocuous image. It can also be used for sending confidential information across mails. Even if the laptop is lost it will be impossible to retrieve this information as the confidential stored in PC is amongst thousands of images stored

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

One important element in the successful implementation is creation of awareness about the user role in security management and use of the new technology. Hence one of the best policies for risk management is to mobilize the various departments of the organization to work together and the inclusion of security as a part of their KRA's.

VII.CONCLUSIONS

Many corporate leaders and senior managers admit the need of securing confidential data and are very interested in information security. Unfortunately, many organizations are not fully aware of the availability of the proposed steganography technology. This proposed approach satisfies the qualities of Confidentiality, Integrity, Availability, Accuracy and Completeness.

Organizations can minimize the business threat of a lost or missing laptop using the proposed method explained in this research paper. To use this approach, organizations will have to write proper policy guidelines to include strict authentication and access procedures, user's role in securing confidential data and conduct training and awareness campaign to safeguard data in the event of laptop being stolen. The primary concern in using steganography image is that the output image is very natural and clear that it does not to raise suspicion. This study also presents a novel steganography technique with the unique property by using LSB technique and increasing data security by employing encryption to the secret information. The research issue is an important future task of this study. Another research task to be considered for the proposed model may exist on how to create awareness and disseminate the technology into corporate entities. Further by empowering the user with a simple tool to hide the existence of information it would be better approach to safeguarding the assets especially for a threat – Loss or stolen laptops.

Thus, the implementation issue is still an important research task for management, along with the technological development as discussed in this article. Finally, it is hoped that this study can be the first step to creating awareness about the availability of new technology related to information security.

REFERENCES

[1] Business Risk of a Lost Laptop A Study of U.S. IT Practitioners Sponsored by Dell Corporation Independently conducted by Ponemon Institute LLC Publication Date: April 2009

[2] Information security management needs more holistic approach: A literature review

Zahoor Ahmed Soomro, Mahmood Hussain Shah ,Javed Ahmed

The business necessity of cybersecurity: It's not an IT issue. Security: Solutions for Enterprise Security Leaders, 51(3), 56.) Chabinsky, S. (2014)

[3] "Applications for Data Hiding." IBM Systmes Journal. Vol 39, Nos. 3 & 4, c. 2000, pgs. 547 – 566. http://www.almaden.ibm.com/cs/people/dgruhl/afdh.pdf

The Challenges of Security Management Richard A. Caralli, William R. Wilson Survivable Enterprise Management Team Networked Systems Survivability Program Software Engineering Institute

[4] Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: lessons from select cases from India and Germany.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[5] Global Journal of Flexible Systems Management, 14(4), 225–239. http://dx.doi.org/10.1007/s40171-013-0047-4)

[6] Http://www.ey.com/Publication/vwLUAssets/Fighting to close the gap: 2012 Global Information Security Survey Fighting to close the gap.pdf. Ernst & Young, 2012(Ernst, Young, (2012)

[7] Employees' adherence to information security policies: An exploratory field study Siponen, Mahmood, & Pahnila, 2014 Siponen, M., Mahmood, M. A., & Pahnila, S. (2014).

[8] Information security management (ISM) practices: lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, 14(4), 225–239.

[9] N. F. Johnson and S. Jajodia, "Exploring steganography : seeing the unseen", IEEE Computer, 31(2), 1998, pp. 26–34.

[10] Gary C.Kessler, "An Overview of Cryptography: Cryptographic", HLAN, ver. 1,1999-2014.

[11] Domenico Bloisi and Luca Iocchi, "IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY", Sapienza University of Rome, Italy, 2002.

[12] Anu Binny and Maddulety Koilakuntla "Hiding Secret Information Using LSB Based Audio Steganography" Soft Computing and Machine Intelligence (ISCMI), 2014 International Conference