# Steganography-covert channels

No body really knew about what Steganography is. Apart from some computer experts, government and military officials' engineers, no body ever cared about it but then its popularity surged after September 11 attacks on United States. This is because it made top brass of intelligence forces believe that the terrorists communicated with each other through hidden or ' covert' messages thus pointing towards steganography (Bialey, 2005).

US officials were so much perplexed by it that they did not knew that their so much efficient and up to date detecting machines failed in unearthing and uncovering such messages which led to such a catastrophic and drastic terrorist attack inside their home land. Through Steganography, messages are sent in such a way that no body can find out the hidden message inside it. In other words the message its self never attracts any other party to come and check it by appearing it to be suspicious. The message is encrypted in such a way that It looks to be harmless for example it is sent through html, jpeg, jpg file formats.

In it there are bits of different and invisible information (Cox, 2007). Why it has the edge over the other encrypted messages is that even if it is deciphered, it is impossible to see the hidden message it has been carrying inside it. As the word ' steno' has been taken from the ancient Greek terminology, it carries its true meaning of having covered message, which cannot be deciphered. Greeks have been using this form of sending covert messages so it shows that the clandestine and covert messages were also there at that point in time.

This shows that the technique is not a new one, it is been carried out from thousands of years but yet, it has been modified to a comparatively higher

level as new encrypting techniques and methodologies with the use of new equipment such as computers and other technological gadgets have made their way into the market. Some of the famous software's which are used for this purpose include White Noise Storm and S- Tools. Similarly Steghide and MP3Stego hide these sorts of messages in the audio, video and mp3 files. These software's enable a person to digitalize the information and embed it in the video, audio or in any still images.

The encryption can never be revealed to the naked human eye. Other soft wares, which are also used, include JP Hide and JP Seek, Blind Side, GIF shuffle, Wb Stego and Stego video (Kipper, 2003). The first one which is JP hide and JP Seek makes a user encrypt a message in the image. On the other hand Blind Side is a special took which does not let anyone know that even a message was passed, so discreet is its movement that it never looked to be suspicious or drew any attention to others. The program GIF shuffle changes the color map of the image (Wayner, 2007). It only works with the GIF images.

It also provides compression and encryption of the concealed message. WB stego on the other hand is one step ahead as it deals with the HTML, adobe PDF and other text files. Lastly, Stego Video hides any message in the video's sequence. It finds empty places in every video format and the bugs the message in it, which is never detected without using steganalysis soft wares. Uses of Covert Channels The usage of stenographic messages was also seen in World War II. Many new were unearthed by the intelligence agencies of United States, notably CIA for example the famous incident of ' Doll Woman'.

What she was to do was to gather and collect information related to American army and their deployments shoring with the news and events related to the US and its allies. After that she used to place order of dolls in such a way which gave a message to the Japanese of what to do or what not to. Also Japanese advancement towards Pearl Harbor in stealth taking Americans with shock and awe strategy and making them go berserk also happened due to the transformation of such encrypted messages from their spys in the United States (Bialey, 2005).

Moreover Allies at that time have banned the transportation of all sorts of materials from their borders because they were afraid that the enemy might not come up with steganographic messages for its spys in their homeland. For this they even banned transportation of all sorts of vegetables, flowers, dates and even stationary. Apart from this, we have seen a lot of covert message activity in Cold War. Both Russians and the Americans have invested heavily in the devising such techniques and tactics of encrypting messages which left both of them in awe and amazement when the cold war finally ended (Wayner, 2007).

The arch rivalry in other terms have made both countries masters of devising such techniques and modes of sending messages which were never used or explored before and gave them an advantage over all other countries as no body never invested so heavily in it. As it uses soft images like pictures and graphics, it has been reported that one thing which irritates and irks FBI and CIA is when Bin Laden goes on internet and start working because it is believed that the terrorists pictures and the information related to their

hideouts and their targets flanked with maps and other information are placed on the internet.

Similarly top spy American agencies agree on that why the names of those terrorists who hit plane on twin towers of world trade center were never there on the flight lists provide by the United and American Airlines (Bialey, 2005). American Spy masters also believe that there is a similar network of steganographic messages between Hizbollah and Hamas, which have created havoc last year by pushing Israel back to its borders. This is also used to smuggle sensitive data out of the firm mainly to rival or competing firms (Kipper, 2003).

A manager can act as a mercenary for the other firm and can send information through stenography to other organization without letting the effected organization know that an important piece of information has been given out which can be anything; it can be related to the company's financials, it can be something related to the innovative product or a plan for a product launch etc. Computer hackers have also been using this technology for years. They have evaded a lot of security checks in the past and have baffled the top spy agencies of the world.

Al Qaeda these days is very active in plaguing the Internet. The CIA and FBI are constantly trying to break their code so they can get to know about their malicious designs and plans against the western powers. Delving down deep into it, if we talk about the terminology, it is no doubt a very interesting one. First there is a payload. A payload is a data, which a sender wants to be transferred to the recipient. It is basically the main thing of the entire

message all else goes irrelevant. Then this payload is hidden into a carrier like JPEG formats or other sound or wave formats.

Steganalysis is the process of unearthing the hidden information inside the file. Redundant bytes on the other hand are those free bytes, which can be encrypted with messages without hurting or damaging the main file. One really asks how the message gets encrypted in audio message. It is done with the technique of echo data hiding. In it low bit encoding is done which can never be heard or noticed by the human ear. In video, Discreet Cosine Transform is done which changes the certain parts of the images, usually rounds them up make it invisible to human eye.

One would be really amazed to know that steganography is also done in documents. It is done in a very crafty way because the risk of going visible is huge. It is done by simply giving more tabs and spaces between the words and makes such a stream of lines, which clearly talk about the message when encrypted. The space and tabs as leave the blank white space, a message can be encrypted into it and the software for it used is SNOW. As all the word related documents have spaces in between them, this is why encryption gets easy in the word documents but the message should be clearly encrypted (Johnson, 2000).

Covert Channels Covert channels on the other hand are the hidden channels that operate while hedging itself on the other network. Steganography is also a type of a covert channel. It mainly draws all its power or bandwidth from it when it has to transit the data. This obviously draws the capacity from the latter whose bandwidth is reduced. One can also say that the system is hacked in this way. In layman terms it acts just like a leech that sticks to the

shark and feeds itself on whatever sharks' feeds on. Covert channel works under the domain of the legitimate communication channel.

The usage of bandwidth tells what sort of steganography message it was i. e. if it has used low bit order of pixel then bandwidth consumer would be less, whereas if it had a high bit order of pixel then the bandwidth consumed would be more. Covert channels put and extra load on the system and they warrant permanent effacement. The transmission of data in this way is already unethical and banned so these covert channels should also be blocked immediately so to prevent user's privacy. This also leads to another concept of port knocking (Johnson, 2000).

As I talked about the steganalysis, it is the unearthing or decoding of a message. It is also known to be an art of detecting the coded messages. Techniques are applied in uncovering those messages, which were suspected to be in coding. One of the techniques is using anti steganographic softwares. Other includes comparing the file with another identical file for example if you have downloaded a JPEG file and suspect it with some message then its identical copy can tell you clearly whether it is encrypted or not as it will probably show a change in size or picture value.

Some of the famous steganalysis tools include Steganography Analyzer Artifact Scanner, Signature Scanner, and Digital Invisible Ink tool kit. Steganography Analyzer Scanner basically scans entire document and individual directories or suspected media material to find the traces of hidden messages. The signature Steganalysis basically looks for the hexadecimal bytes or signatures hidden in the file. Like wise the invisible ink

tool kit decrypts a message inside a 24-bit color image accompanied by the performance of a statistical analysis.

As I have mentioned, the steganalysis is mainly handled with statistical analysis. These statistical analyses basically are there to find inconsistencies in the data mainly to highlight the way it has been organized. Detection becomes really difficult when there is a single image available because then one has to make attempts to see what was the original picture and what changes have been brought into it. Carrier noise plays a very important part over here as it tells the decoder whether the file was encrypted or not.

The trouble for the decryptor never ends over here, what if the payload has been encrypted first and then inserted into the file? Now this creates a lot of issues, as you have to see things in more detail and with more scrutiny being vigilant of even small blips and movements in the pixels. If the pay load is encrypted the noise looks to be more disturbed in the message which is then hard to be deciphered because the decryptor has to first decode the carrier and then the payload. Stega Analysis and Efficiency

As I have said earlier, stenography’s detection tools are also available. The most efficient or current detection methods include detection through magic bytes, character distribution and file extension. As every method or tool has its strengths and weaknesses, these methods have also their strengths and weaknesses. In magic bytes, files are detected by bytes and by matching signatures (Cox, 2007). These signatures vary in length. As the graphic formats such as JPG or JPEG have different color pallets they are associated with different file types and extensions.

Once the bytes are analyzed, they are then compared with the actual ones or most precisely what the software program has expected it to be for example, if the file is JPG, it should be JPG instead of being JPEG. If the latter happens then a red flag is raised. The main problem with this sort of a technology is that it only works on binary files types. This implies that only those files will be checked who have the same type (the type which has been stored in the program to be checked). The problem becomes magnified when the malicious and notorious content from Linux or C++ coded files are left unchecked (Shih, 2007).

Another weakness is that magic bytes cannot enforce or regulate different ‘ types’ of files because they are not going to follow the standards when editing or tailoring the files. In character distribution what happens is that American Standard Code for information interchange, ASCII is examined. The method is gives a tally result, which leads to the different distributions and making of histograms. Like Magic numbers fails to detect the java scripts, the distribution of characters do reveal whether the file is coded with data or not.

File detection through characters has also a weak point because it can raise unnecessary alarms on interpreting the irregular or weak content. Now lastly the file extension, it is not that reliable as the other two are but still holds its importance in the detection of coded messages. The method which is being applied over here is amateurish as all is dependent on the file name i. e. if file name is changed then it is encrypted but this is one of the weakest signals as file’s properties can be changed by some mouse clicks and key strokes (Cox, 2007).