



TIPS FOR NEGOTIATING

The ability to negotiate successfully in today's turbulent business climate can make the difference between success and failure. These are some tips for negotiating your clients and gain a win-win situation.

1. Don't be afraid to ask for what you want: Successful negotiators are assertive and challenge everything – they know that everything is negotiable. I call this negotiation consciousness. Being assertive means asking for what you want and refusing to take NO for an answer. Practice expressing your feelings without anxiety or anger. Let people know what you want in a non-threatening way. Practice 'I' statements.

2. Shut up and listen: I am amazed by all the people I meet who can't stop talking. Negotiators are detectives. They ask probing questions and then shut up. The other negotiator will tell you everything you need to know – all you have to do is listening. Many conflicts can be resolved easily if we learn how to listen. The catch is that listening is the forgotten art. You can become an effective listener by allowing the other person to do most of the talking. Follow the 70/30 Rule – listen 70 percent of the time, and talk only 30 percent of the time.

3. Do your homework: Gather as much pertinent information prior to your negotiation. What are their needs? What pressures do they feel? What options do they have? Doing your homework is vital to successful negotiation. You can't make accurate decisions without understanding the other side's situation. The more information you have about the people with whom you are negotiating, the stronger you will be. People who consistently leave money on the table probably fail to do their homework.

4. Always be willing to walk away: Never negotiate without options. If you depend too much on the positive outcome of a negotiation, you lose your ability to say NO. When you say to yourself, "I will walk if I can't conclude a deal that is satisfactory," the other side can tell that you mean business. Your resolve will force them to make concessions.

5. Don't be in a hurry: Being patient is very difficult for us. We want to get it over with. More flexible about time has the advantage. Your patience can be devastating to the other negotiator if they are in a hurry because they start to believe that you are not under pressure to conclude the deal. So what do they do? They offer concessions as a means of providing you with an incentive to say YES.

6. Aim high and expect the best outcome: Successful negotiators are optimists. A proven strategy for achieving higher results is opening with an extreme position. Your optimism will become a self-fulfilling prophecy. Conversely, if you have low expectations, you will probably wind up with a less satisfying outcome.

7. Focus on the other side's pressure, not yours: We have a tendency to focus on our own pressure, on the reasons why we need to make a deal. It's the old story about the grass being greener in the other person's backyard. If you fall into this trap, you are working against yourself. The other side will appear more powerful. When you focus on your own limitations, you miss the big picture. It's your job to be a detective and root these out. If you discover that they are under pressure, which they surely are, look for ways to exploit that pressure in order to achieve a better result for yourself.

8. Show the other person how their needs will be met: Successful negotiators always look at the situation from the other side's perspective. Everyone looks at the world differently, so you are way ahead of the game if you can figure out their perception of the deal. Instead of trying to win the negotiation, seek to understand the other negotiator and show them ways to feel satisfied. Satisfaction means that their basic interests have been fulfilled, not that their demands have been met.

9. Don't give anything away without getting something in return: Unilateral concessions are self-defeating. Whenever you give something away, get something in return. When you give something away without requiring them to reciprocate, they will feel entitled to your concession, and won't be satisfied until you give up even more.

10. Don't take the issues or the other person's behavior personally: All too often negotiations fail because one or both of the parties get sidetracked by personal issues unrelated to the deal at hand. Successful negotiators focus on solving the problem. Obsessing over the other negotiator's personality, or over issues that are not directly pertinent to making a deal, can sabotage a negotiation. If someone is rude or difficult to deal with, try to understand their behavior and don't take it personally.

□□□

Courtesy by: Prof. Ed Brodow is an internationally renowned expert.

DIGITAL IMAGE STEGANOGRAPHY

By: ¹Prof. Akhil Khare, ²Meenu Kumari, ³Pallavi Khare

Abstract:

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images. Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

KEYWORDS: Steganography, Out Guess Steganography algorithm, Statistical Steganography.

1. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. Today, the term steganography includes the concealment of digital information within computer files. For example, the sender might start with an ordinary-looking image file, and then adjust the color of every 100th pixel to correspond to a letter in the alphabet -- a change so subtle that no one who isn't actively looking for it is likely to notice it.

The word steganography is of Greek origin and means "covered, or hidden writing". Its ancient origins can be traced back to 440 BC. Herodotus mentions two examples of steganography in the histories of Herodotus. Demeratus sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax. Wax tablets were in common use then as re-usable writing surfaces, sometimes used for shorthand. Another ancient example is that of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the Persians. Later, Johannes Trithemius's book Steganographia is a treatise on cryptography and steganography disguised as a grimoire.

Generally, a steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message. This apparent message is the cover text. For instance, a message may be hidden by using invisible ink between the visible lines of innocuous documents.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in countries where encryption is illegal.

Steganography used in electronic communication include steganographic coding inside of a transport layer, such as an MP3 file, or a protocol, such as UDP.

2. LITERATURE SURVEY

We are living in an age of science. Communication has become major part of our daily life today. With the increasing communication traffic demand, data security has become very important field [2].

Lots of data security and data hiding algorithms have been developed in the last decade. In this project we are implementing a method of "Digital Stenography" for image data hiding [5].

Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file [6].

A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption [9].

3. MAIN FUNCTIONALITIES

Digital image steganography system is a stand-alone application that combines steganography and encryption to enhance the confidentiality of intended message. The user's intended message is first encrypted to create unintelligible cipher text. Then the cipher text will be hidden within an image file in such a way as to minimize the perceived loss in quality. The recipient of the image is able to retrieve the hidden message back from the image with this system.

¹ Assistant Professor, Department of Information Technology, Bharati Vidyapeeth College Of Engineering, Pune, India.

² Research Student, Department of Information Technology, Bharti Vidyapeeth College Of Engineering, Pune, India.

³ Research Student, Department of E&TC, SSSIST Bhopal, India

3.1 Encoding

In order to hide text in an image, the user must provide the text and a Target Image in which it is to be hidden. Optionally, users may enter or load a text key. When a user key is not provided, a default key is used. To make choosing images easier, an image bar is provided for the user. The user may set the source directory, whose contents are displayed as thumbnails in the image bar located on the bottom panel of application. These thumbnails are automatically generated from the specified source directory. The user then selects a target image and loads it for use as the Target Image. The user may also open the Target Image by selecting Open Image under File menu. The user may enter the text to be embedded in several ways. He or she may type it directly into the text window, open a text file, or paste text from another application. The user may also open a text file by selecting Open Text under the File menu or use the Edit menu to paste from the clipboard. Loading a text key can be done from the Open Text Key selection on the Tools menu. When user has specified both the target image, and text body, Digital image steganography system is ready to hide the text body within the image. The user may then select Embed Text from the Tools menu. The key image will then be hashed into an appropriate Key Value. This value will be used for the encryption of the user's plaintext to produce cipher text. The cipher text and key value will then be input into the steganography and bit placement algorithms, and the Output Image will be generated. After the application has generated the image, the user may then inspect it by selecting the Image tab on the main panel. The user is then able to compare the encrypted target image with the original target image located on the right box of the main window. The user may wish to save the generated image by selecting Save Image or Save Image As... under File menu.

3.2 Decoding

In order to retrieve the hidden text from a source image, the user needs to provide a Source Image and any Keys used when the Source Image was generated. Loading the Source Image file is done similarly to the process of opening a Target Image. If the sender has used the default key, the recipient need not load any keys to the application. If a non-default key was used in text hiding process, the receiving party must have prearranged knowledge of the key for use in retrieving the text. This key could be text file or a key string. If the key is a text file, the user may load the key by selecting Open Text Key from the Tools menu. Lastly, the user may simply type in the key by activating the Text tab of the key panel and entering it. After the Source Image and any required Keys are loaded into the application, the hidden text can be retrieved by selecting Extract Text from the Tools menu. The key will be hashed into an appropriate Key Value. This key

value will be used to recover the hidden cipher text from the Source Image. The key will then be used for the decryption of the cipher text to produce plaintext. The plaintext will finally be displayed in the text box on the Text tab of the main panel. After the application has generated the text, the user may wish to save the generated text by selecting Save Text under the File menu. The application is not able to identify the presence of the hidden message in images until the actual decoding process is attempted, as the image files are virtually indistinguishable from normal images.

4. STEGANOGRAPHIC TECHNIQUES

Modern Steganography entered the world in 1985 with the advent of the Personal Computer applied to classical steganography problems. Development following that was slow, but has since taken off, based upon the number of 'stego' programs available.

- ✧ Concealing messages within the lowest bits of noisy images or sound files.
- ✧ Concealing data within encrypted data. The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data. This technique works most effectively where the decrypted version of data being overwritten has no special meaning or use: some cryptosystems, especially those designed for file systems, add random looking padding bytes at the end of a cipher text so that its size cannot be used to figure out the size of the original plaintext. Examples of software that use this technique include Free OTFE and True Crypt.
- ✧ Chaffing and winnowing
- ✧ Invisible ink
- ✧ Null ciphers
- ✧ Concealed messages in tampered executable files, exploiting redundancy in the i386 instruction set.
- ✧ Embedded pictures in video material (optionally played at slower or faster speed).

5. DIFFERENT KINDS OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display without the alteration being done. Figure 5.1 shows the four main categories of file formats that can be used for steganography.

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is

only since the beginning of the Internet and all the different digital file formats that is has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

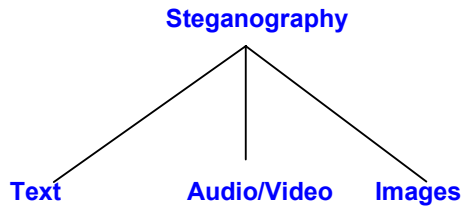


Fig. 5.1: Categories of Steganography

Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography. To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images. The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

6. IMAGE STEGANOGRAPHY ALGORITHM

The JPEG format is currently the most common format for storing image data. It is also supported by virtually all software applications that allow viewing and working with digital images. LSBs of After Embedding the image is processed again using a second pass. . Because chi-square attack is based on it.

6.1 Breaking Outguess

The OutGuess steganographic algorithm was proposed by Neils Provos to counter the statistical chi-square attack. In the first pass, similar to J-Steg, OutGuess embeds message.

- Outguess Preserves the histogram of DCT coefficients exactly.
- Outguess cannot be detected using the chi – square attack or its generalized versions.
- Modifies LSBs of DCT coefficients at random locations. Corrects statistical deviation by modifying unused LSBs.

- Distribution of DCT coefficients is preserved after embedding process.

The main feature of outguess is that outguess hides messages in JPEG files and it embeds hides messages in bits in LSBs of quantized DCT coefficients along a key –dependent walk through the image.

6.2 Algorithm for Encoding

- 1) The input is a Buffered Image object, which contains a Color Model and a matrix representing the image with pointers aimed at indices of the Color Model. The RGB values of the uncompressed input image are converted into three components: one luminance component and two chrominance components (YUV). The luminance component is considered more important.
- 2) The image is separated into 8x8 pixels blocks starting from the upper left-hand corner.
- 3) The component signals for each 8x8 block are transformed into the frequency domain by using the two-dimensional discrete cosine transform (DCT). This transformation is similar to the two-dimensional fast Fourier transformation.
- 4) While the coefficients closest to 0 are eliminated, the remaining coefficients are quantized using various degrees of accuracy. This can be modified by changing the quantization tables. The DC luminance coefficients are the most important and are quantized with the most accuracy.

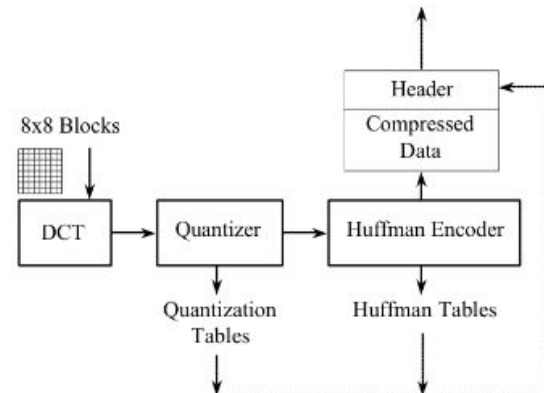


Fig. 6.2.1 Block Diagram of Algorithm

6.3 Algorithm for Decoding

The decoding scheme is much simpler than encoding. The averages of the luminance of the 8x8 blocks just need to be calculated and converted back to bits. Basically what we exactly do in decoding process is:-

- 1) The user needs to provide a Source Image and any keys used when the Source Image was generated.
- 2) If a non-default key was used in text hiding process, the receiving party must

have prearranged knowledge of the key for use in retrieving the text.

- 3) After the Source Image and any required keys are loaded into the application, the hidden text can be retrieved by selecting Extract Text from the Tools menu.

7. CONCLUSIONS AND FUTURE DEVELOPMENTS

7.1 Future Development

The application is primarily intended to be used to inconspicuously hide confidential and proprietary information by anyone seeking to hide information. This software has an advantage over other information security systems because the hidden texts are in the form of image, which are not obvious text information carriers.

Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program.

Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

Digital Image Steganography system allows a user to securely transfer a text message by hiding it in a digital image file. 128 bit AES encryption is used to protect the content of the text message even if its presence were to be detected. Currently, no methods are known for breaking this kind of encryption within a reasonable period of time (i.e., a couple of years). Additionally, compression is used to maximize the space available in an image.

To send a message, a source text, an image in which the text should be embedded, and a key are needed. The key is used to aid in encryption and to decide where the information should be hidden in the image. A short text can be used as a key.

7.2 Conclusions

The meaning of Steganography is hiding information and the related technologies. There is a principal difference between Steganography and Encryption; however they can meet at some points too. They can be applied together, i.e. encrypted information can be hidden in addition. To hide something a covering medium is always needed. The covering medium must be redundant; otherwise the hidden information

could be detected easily. The technology of hiding should match the nature of the medium. The hidden information should not be lost, if the carrying medium is edited, modified, formatted, re-sized, compressed or printed. That's a difficult task to realize. It's an expectation as well, that the fact of hidden information should be impossible to detect by other than the addressee. On the other hand security services should have methods to detect such information. At least its existence. Realizing a wood trade-off there are different technologies. Nowadays the most popular application of Steganography is hiding copy rights and other commercial information. Such kind of hidden information is known as e-watermark. The e-watermark is not always invisible. There are cases when it is made deliberately strikingly visible. e.g. in case of trial versions of software.

REFERENCES

- [1] N. Provos, "Defending Against Statistical Steganography," Proc 10th USENEX Security Symposium 2005.
- [2] N. Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.
- [3] S. Katzenbeisser and Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking" Artech House, Norwood, MA. 2000.
- [4] L. Reyzen And S. Russell, "More efficient provably secure Steganography" 2007.
- [5] S.Lyu and H. Farid , "Steganography using higher order image statistics , " IEEE Trans. Inf. Forens. Secur. 2006.
- [6] Venkatraman, S, Abraham, A. & Paprzycki M. "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and computing, 2004.
- [7] Fridrich, J., Goljan M., and Hogeia, D; New Methodology for Breaking stenographic Techniques for JPEGs. "Electronic Imaging 2003".
- [8] http://aakash.ece.ucsb.edu/~data_hiding/stegdemon.aspx.Ucsb data hiding online demonstration. Released on Mar .09,2005.
- [9] Mitsugu Iwanmoto and Hiroshuke Yamamoto, "The Optimal n-out-of-n Visual Secret Sharing Scheme for GrayScale Images", IEICE Trans. Fundamentals, vol.E85-A, No.10, October 2002, pp. 2238-2247.
- [10] Doron Shaked, Nur Arad, Andrew Fitzhugh, Irwin Sobel, "Color Diffusion:
- [11] Error Diffusion for Color Halftones", HP Laboratories Israel, May 1999.
- [12] Z.Zhou, G.R.Arce, and G.Di Crescenzo, "Halftone Visual Cryptography", IEEE Tans. On Image Processing, vol. 15, No..8, August 2006, pp. 2441-2453



REMOTE CONTROLLERS—A NEW WAY OF LIFE

By: MANU AHUJA, Lecturer, Orissa Engineering College, Bhubaneswar

Continued from May, 2010 issue....

Among the main developments is the inclusion of Zig Bee controllers in Sony's and Panasonic's higher-end flat-screen TVs. Uptake by the A/V industry is crucial if Zig Bee is really to take off in the home. But the ZigBee Alliance needs to start educating consumers about ZigBee. It promises many advantages over existing remote control solutions, including richer communication and increased reliability, enhanced features and flexibility, interoperability, and no line-of-sight barrier. The ZigBee Alliance, the standards body that defines ZigBee, also publishes application profiles that allow multiple OEM vendors to create interoperable products. The current list of application profiles either published or in the works are: Home Automation, ZigBee Smart Energy 1.0/2.0, Commercial Building Automation, Telecommunication Applications, Personal, Home, and Hospital Care & Toys. The relationship between IEEE 802.15.4 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The ZigBee 1.0 specification was ratified on 14 December 2004 and is available to members of the ZigBee Alliance.

Most recently, the ZigBee 2007 specification was posted on 30 October 2007. The first ZigBee Application Profile, Home Automation, was announced 2 November 2007. As amended by NIST, the Smart Energy Profile 2.0 specification will remove the dependency on IEEE 802.15.4. Device manufacturers will be able to implement any MAC/PHY, such as IEEE 802.15.4(x) and IEEE P1901, under an IP layer based on 6 Low PAN. ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and less expensive than other WPANs such as Bluetooth.

Zig Bee chip vendors typically sell integrated radios and microcontrollers with between 60K and 128K flash memory, such as the Jennic JN5148, the Free scale MC13213, the Ember EM250, the Texas Instruments CC2430, the Samsung Electro-Mechanics ZBS240 and the Atmel ATmega128RFA1. Radios are also available stand-alone to be used with any processor or microcontroller. Generally, the chip vendors also offer the ZigBee software stack, although independent ones are also

available. As ZigBee can activate (go from sleep to active mode) in 15 msec or less, the latency can be very low and devices can be very responsive — particularly compared to Bluetooth wake-up delays, which are typically around three seconds. As Zig Bees can sleep most of the time, average power consumption can be very low, resulting in long battery life.

TYPES

There are three different types of ZigBee devices:

ZigBee coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally. It is able to store information about the network, including acting as the Trust Centre & repository for security keys.

ZigBee Router (ZR): As well as running an application function, a router can act as an intermediate router, passing on data from other devices.

ZigBee End Device (ZED): Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.

USES

ZigBee protocols are intended for use in embedded applications requiring low data rates and low power consumption. Zig Bee's current focus is to define a general-purpose, inexpensive, self-organizing mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc. The resulting network will use very small amounts of power — individual devices must have a battery life of at least two years to pass ZigBee certification.

The typical application areas are:-

- a) Home Entertainment and Control — Smart lighting, advanced temperature control, safety and security, movies and music.
- b) Home Awareness — Water sensors, power sensors, energy monitoring, smoke and fire detectors, smart appliances and access sensors.
- c) Mobile Services — m-payment, m-monitoring and control, m-security and access control, m-healthcare and tele-assist.
- d) Commercial Building — Energy monitoring, HVAC, lighting, access control.
- e) Industrial Plant — Process control, asset management, environmental management, energy management, industrial device control. [5]

BLUETOOTH TECHNOLOGY

Bluetooth is a proprietary open wireless electronic protocol for exchanging data over short distances (using short length radio waves) from fixed and mobile devices, creating personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Bluetooth is a standard communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 100 m, 10 m and 1 m, but ranges vary in practice) based on low-cost transceiver microchips in each device. As the devices use a radio (broadcast) communications system, they do not have to be in line of sight of each other. The versions of this technology are Bluetooth 1.0 and 1.0B,, Bluetooth 1.1,, Bluetooth 1.2,, Bluetooth 2.0 + EDR,, Bluetooth 2.1 + EDR,, Bluetooth 3.0 + HS,, Bluetooth V4.0 (BLE; low energy protocols).

Bluetooth uses Radio Frequency Spectrum & has two-way communication which gives you the ability to create intelligent remote controls. The picture of a future remote control that incorporates Bluetooth technology: Imagine having picture-in-picture on your remote in a little preview window. Instead of taking up the whole screen while flipping through channels to find out what's on, you can preview it on a little video screen on the Bluetooth remote without annoying the other people in the room. This is all possible with Bluetooth technology. Bluetooth can handle many times as compared to the quality of video that you can stream over the Internet. To make this happen, Bluetooth needs to work with set-top box manufacturers and/or TV manufacturers.

IMPLEMENTATION

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 bands of 1 MHz width in the range 2402-2480 MHz. This is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band. In its basic rate (BR) mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross data rate of 1 Mbit/s. In extended data rate (EDR) $\pi/4$ -DQPSK and 8 DPSK are used, giving 2, and 3 Mbit/s respectively.

Bluetooth is a packet-based protocol with a master-slave structure. One master may communicate with up to 7 slaves in a piconet; all devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 μ s intervals. Two clock ticks make up a slot of 625 μ s; two slots make up a slot pair of 1250 μ s. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots; the slave, conversely, receives in even slots and transmits in odd slots.

Bluetooth provides a secure way to connect and exchange information between devices such as faxes, mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles. The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG consists of companies in the areas of telecommunication, computing, networking, and consumer electronics.[To be marketed as a blue tooth device, it must be qualified to standards defined by the SIG.

APPLICATIONS

- 1) Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- 2) Wireless networking between PCs in a confined space and where little bandwidth is required.
- 3) Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- 4) Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.

- 5) For controls where infrared was traditionally used.
- 6) For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- 7) Three seventh-generation game consoles, Nintendo's Wii and Sony's PlayStation 3 and PSP Go, use Bluetooth for their respective wireless controllers.
- 8) Dial-up internet access on personal computers using a data-capable mobile phone as a wireless modem like Novatel WiFi.
- 9) Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated tele health devices.

Bluetooth is intended for non-resident equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any ambience.

FUTURE PROSPECTS

- 1) Broadcast channel—this will enable the Bluetooth information points. It will drive the adoption of Bluetooth into mobile phones and enable advertising models based around users pulling information from the information points, and not based around the object push model that is used in a limited way today.
- 2) Topology management—it will enable the automatic configuration of the piconet topologies especially in scatternet situations that are becoming more common today. This should all be invisible to users of the technology, while also making the technology "just work."
- 3) QoS improvements— these will enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet. [6]

CONCLUSION

With the advent of technology, today remote controllers have become an essential part of our life may be entertainment electronics, household appliances or other devices. However, we have to be careful that these are not misused.

Remote Controllers have come a long way ever since they were first designed by N. Tesla in the year 1898.

There have been many upgrades in the technology from Radio control to ultrasonic control to laser control to infrared control to the presently developed universal remote control. The future trends in the area will be based on new electronic protocols such as Bluetooth Wireless USB and Zigbee for development of self learning and intelligent remote control for household and industrial applications.

References

- 1) Julie Moyer, Patrick Ott and David Pearson, Webpage on "All about Remote Control" 29 January, 1999, library.thinkquest.org/25304/index.html.
- 2) "Five Decades of Channel Surfing: History of TV Remote Control" .Archived from the www.zenith.com.
- 3) "Remote Control" World Book Encyclopedia, Chicago: World Book Inc. 1990
- 4) "Remote Manipulators" Mc Graw Hill Encyclopedia of Science and Technology. New York: Mc Graw Hill Publishers, 1997.
- 5) Zigbee – Wikipedia, the free Encyclopedia, en.wikipedia.org/wiki/zigbee
- 6) Bluetooth – Wikipedia, the free Encyclopedia, en.wikipedia.org/wiki/bluetooth
- 7) Remote Control Wikipedia, the free Encyclopedia, from en.wikipedia.org/wiki/remote_control.



ARTICLES

Readers are requested to send articles for publishing in NAFEN DIGEST on the latest areas of:

- ✧ **Management**
- ✧ Finance
- ✧ **Engineering**
- ✧ Information Technology
- ✧ **Science & Technology**

Through e-mail: nafenindia@nafenindia.com or nafenindia@airtelmail.in preferably in M.S. Word.

Selected Best Article for year 2010-2011 will be suitably awarded by NAFEN.

NAFEN MEMBERSHIP

For Individual/ Fellow/ Life / Corporate Membership of National Foundation of Indian Engineers (NAFEN) log on www.nafenindia.com and Register yourself ONLINE or contact NAFEN SECRETARIAT.

Members Derive following Advantages:

- ❖ Very low Delegate Fee for participation in International events of NAFEN.
- ❖ Chances of participation in various NAFEN events in India & abroad.
- ❖ Scholarships for meritorious students for studies in India & abroad.
- ❖ More Exposure in emerging areas rather than only on Technical aspects.
- ❖ Chances to meet leaders of corporate world more frequently, that is, people who matter.

DIGEST EDITORIAL BOARD

Dr. P. K. Gupta	-	Editor
Mr. Rishi Kumar	-	Jt. Editor
Dr. A.P. Kulshreshtha	-	Member
Prof. P. B. Sharma	-	Member
Dr. S.K. Jha	-	Member
Mr. R.M. Verma	-	Member

**Online Comments/ Suggestions
welcome at**

**National Foundation of Indian
Engineers**

Web: www.nafenindia.com or
E-mail: nafenindia@nafenindia.com
nafenindia@airtelmail.in