ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation

P.Sudha[1], R.Radha[2]

M. Phil Scholar, Department of Computer Science and Research, Bharathiyar Arts and Science College (w), Deviyakurichi , Attur (tk),Salem(dt) , Tamil Nadu,India[1].

Assistant Professor, Department of Computer Science and Research, Bharathiyar Arts and Science College (w), Deviyakurichi , Attur (tk),Salem(dt), Tamil Nadu,India[2].

ABSTRACT: This work proposes a novel reversible image data hiding (RIDH) scheme over encrypted domain. The data embed-ding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non-encrypted image patches, allowing us to jointly decode the embedded message and the original image signal.
The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.
Compared with the state-of-the-arts, the proposed approach provides higher embedding capacity,and is able to perfectly reconstruct the original image as well as the embedded message. Extensive experimental results are provided to validate the superior performance of our scheme.

I. INTRODUCTION

NETWORK SECURITY

In the world of computers, **networking** is the practice of interfacing two or more computing devices with each other for the purpose of sharing data. Computer networks are built with a combination of hardware and software.

Area Networks

Computer networks can be categorized in several different ways. One approach defines the type of network according to the geographic area it spans.

Local area networks (LANs), for example, typically span a single home, school, or small office building, whereas wide area networks (WANs), reach across cities, states, or even across the world. The Internet is the world's largest public WAN.

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common types of area networks are:

- LAN - Local Area Network
- WAN - Wide Area Network
- WLAN - Wireless Local Area Network
- MAN - Metropolitan Area Network
- SAN - Storage Area Network, System Area Network, Server Area Network, or sometimes Small Area Network
- CAN - Campus Area Network, Controller Area Network, or sometimes Cluster Area Network
- PAN - Personal Area Network
- LAN and WAN are the two primary and best-known categories of area networks, while the others have emerged with technology advances.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

LAN - Local Area Network

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.

In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

WAN - Wide Area Network

As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth.

A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN.

In IP networking, the router maintains both a LAN address and a WAN address. A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management.

WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

LAN, WAN and Home Networking

Residences typically employ one LAN and connect to the Internet WAN via an Internet Service Provider (ISP) using a broadband modem.

The ISP provides a WAN IP address to the modem, and all of the computers on the home network use LAN (so-called *private*) IP addresses.

All computers on the home LAN can COMMUNICATE directly with each other but must go through a central network gateway, typically a broadband router, to reach the ISP.

Other Types of Area Networks

While LAN and WAN are by far the most popular network types mentioned, you may also commonly see references to these others:

- **Wireless Local Area Network** - a LAN based on Wi-Fi wireless network technology
- **Metropolitan Area Network** - a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.
- **Campus Area Network** - a network spanning multiple LANs but smaller than a MAN, such as on a university or local business campus.
- **Storage Area Network** - connects servers to data storage devices through a technology like Fiber Channel.
- **System Area Network** (also known as Cluster Area Network).- links high-performance computers with high-speed connections in a cluster configuration.

Network Design

Computer networks also differ in their design approach. The two basic forms of network design are called client/server and peer-to-peer. Client-server networks feature centralized server computers that store email, Web pages, files and or applications.

On a peer-to-peer network, conversely, all computers tend to support the same functions. Client-server networks are much more common in business and peer-to-peer networks much more common in homes.

A network topology represents its layout or structure from the point of view of data flow. In so-called bus networks, for example, all of the computers share and COMMUNICATE across one common conduit, whereas in a star network, all data flows through one centralized device. Common types of network topologies include bus, star, ring networks and mesh networks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Network Protocols

Communication languages used by computer devices are called network protocol. Yet another way to classify computer networks is by the set of protocols they support. Networks often implement multiple protocols with each supporting specific applications.

Purpose of Network Protocols

Without protocols, devices would lack the ability to understand the electronic signals they send to each other over network connections. Network protocols serve these basic functions:

- Address data to the correct recipient(s)
- Physically transmit data from source to destination, with security protection if needed
- Receive messages and send responses appropriately
- Consider a comparison between network protocols with how a postal service handles physical paper mail.

Common Types of Network Protocols

No one protocol exists that supports all the features every kind of computer network needs. Many different kinds of network protocols have been invented over the years, each attempting to support certain kinds of network COMMUNICATION.

Three basic characteristics that distinguish one type of protocol from another are:

- **Simplex *vs.* Duple:** A simplex connection allows only one device to transmit on a network. Conversely, duplex network connections allow devices to both transmit and receive data across the same physical link.
- **Connection-oriented or connection-less:** A connection-oriented network protocol exchanges (a process called a handshake*)* address information between two devices that allows them to carry on a conversation (called a session*)* with each other.
- Conversely, connection-less protocols deliver individual messages from one point to another without regard for any similar messages sent before or after (and without knowing whether messages are even successfully received).
- **Layer:** Network protocols normally work together in groups (called stacks because diagrams often depict protocols as boxes stacked on top of each other).
- Some protocols function at lower layers closely tied to how different types of wireless or network cabling physically works. Others work at higher layers linked to how network applications work, and some work at intermediate layers in between.

Home Networking

While other types of networks are built and maintained by engineers, home networks belong to ordinary homeowners, people often with little or no technical background. Various manufacturers produce broadband router hardware designed to simplify home network setup.

Home broadband routers allow devices in different rooms to efficiently share a broadband Internet connection, enable people to more easily share their files and printers within the network, and help with overall network security.

Home networks have increased in capability with each generation of new technology. Years ago, people commonly set up their home network just to connect a few PCs, share some DOCUMENTS and perhaps a printer. Now its common for households to also network game consoles, digital video recorders, and smart phones for streaming sound and video.

Home automation systems have also existed for many years, but these too have grown in popularity more recently with practical systems for controlling lights, digital thermostats and appliances.

Business Networks

Small and home office (SOHO) environments use similar technology as found in home networks. Businesses often have additional data storage, and security requirements that require expanding their networks in different ways, particularly as the business gets larger.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Whereas a home network generally functions as one LAN, a business tends to contain multiple LANs.

Companies with buildings in multiple locations utilize wide-area networking to connect these branch offices together. Though also available and used by some households, voice over IP communication and network storage and backup technologies are prevalent in businesses.

Larger companies also maintain their own internal Web sites, called intranets to help with employee business communication.

Networking and the Internet

The popularity of computer networks sharply increased with the creation of the World Wide Web (WWW) in the 1990s. Public Web sites, peer to peer (P2P)FILE SHARING systems, and various other services run on Internet servers across the world.

Wired versus Wireless Networking

Many of the same network protocols, like TCP/IP, work in both wired and wireless networks. Networks with Ethernet cables predominated in businesses, schools, and homes for several decades.

More recently, however, wireless alternatives have emerged as the premier technology for building new computer networks, in part to support smart phones and the other new kinds of wireless gadgets that have triggered the rise of mobile networking.Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client.

The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

II. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

The majority of the existing RIDH algorithms are designed over the plaintext domain, namely, the message bits are embedded into the original, un-encrypted images.

The early works mainly utilized the lossless compression algorithm to compress certain image features, in order to vacate room for message embedding. However, the embedding capacity of this type of method is rather limited and the incurred distortion on the watermarked image is severe.

Histogram shifting (HS)-based technique, initially designed, is another class of approach achieving better embedding performance through shifting the histogram of some image features.

DISADVANTAGES

- As local smoothness does not always hold for natural images, data extraction errors can be observed in the high-activity regions.
- Further, Zhang proposed a separable RIDH method such that the protection scopes of data hiding key and encryption key are gracefully separated.
- In extended the lossless compression based RIDH approach to the encrypted domain, namely, losslessly compress half of the 4th LSBs of the encrypted image via LDPC code to create space for data hiding.

2.2 PROPOSED SYSTEM

We propose an encrypted-domain RIDH scheme by specifically taking the above-mentioned design preferences into consideration.

The proposed technique em-beds message through a public key modulation mechanism, and performs data extraction by exploiting the statistical dis-tinguishability of encrypted and non-encrypted image blocks.

Since the decoding of the message bits and the original image is tied together, our proposed technique belongs to the category of non-separable RIDH solutions.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Compared with the state-of-the-arts, the proposed approach provides higher em-bedding capacity, and is able to achieve perfect reconstruction of the original image as well as the embedded message bits.
Extensive experimental results on 100 test images validate the superior performance of our scheme.

ADVANTAGES

- We propose an encrypted-domain secure RIDH scheme without data hiding key.
- As will be clear shortly, the possibility of eliminating the data hiding key is not unique to our proposed method, but rather applicable for all non-separable RIDH schemes.
- Here, some design goals are slightly different from those of the existing solutions, due to the elimination of the data hiding key.

III. LITERATURE SURVEY

A. OVERVIEW

Reversible image data hiding (RIDH) is a special category of data hiding technique, which ensures perfect reconstruction of the cover image upon the extraction of the embedded message. The reversibility makes such image data hiding approach particularly attractive in the critical scenarios, e.g., military and remote sensing, medical images sharing, law forensics and copyright authentication, where high fidelity of the reconstructed cover image is required.

The majority of the existing RIDH algorithms are designed over the plaintext domain, namely, the message bits are embedded into the original, un-encrypted images. The early works mainly utilized the lossless compression algorithm to compress certain image features, in order to vacate room for message embedding

3.1 A NOVEL REVERSIBLE DATA HIDING SCHEME BASED ON TWO-DIMENSIONAL DIFFERENCE-HISTOGRAM MODIFICATION

In this project, based on two-dimensional difference- histogram modification, a novel reversible data hiding (RDH) scheme is proposed by using difference-pair-mapping (DPM). First, by considering each pixel-pair and its context, a sequence consisting of pairs of difference values is computed. Then, a two-dimensional difference-histogram is generated by counting the frequency of the resulting difference-pairs.

Finally, reversible data embedding is implemented according to a specifically designed DPM. Here, the DPM is an injective mapping defined on difference-pairs. It is a natural extension of expansion embedding and shifting techniques used in current histogram-based RDH methods. By the proposed approach, compared with the conventional one-dimensional difference-histogram and one-dimensional prediction-error-histogram-based RDH methods, the image redundancy can be better exploited and an improved embedding performance is achieved.

Moreover, a pixel-pair-selection strategy is also adopted to priory use the pixel-pairs located in smooth image regions to embed data.

This can further enhance the embedding performance. Experimental results demonstrate that the proposed scheme outperforms some state-of-the-art RDH works.

3.2 AN INPAINTING-ASSISTED REVERSIBLE STEGANOGRAPHIC SCHEME USING A HISTOGRAM SHIFTING MECHANISM

In this project, we propose a novel prediction-based reversible steganographic scheme based on image in painting. First, reference pixels are chosen adaptively according to the distribution characteristics of the image content. Then, the image in painting technique based on partial differential equations is introduced to generate a prediction image that has similar structural and geometric information as the cover image.

Finally, by using the two selected groups of peak points and zero points, the histogram of the prediction error is shifted to embed the secret bits reversibly. Since the same reference pixels can be exploited in the extraction procedure, the embedded secret bits can be extracted from the stego image correctly, and the cover image can be restored losslessly.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

Through the use of the adaptive strategy for choosing reference pixels and the in painting predictor, the prediction accuracy is high, and more embeddable pixels are acquired. Thus, the proposed scheme provides a greater embedding rate and better visual quality compared with recently reported methods.

3.3 REVERSIBLE DATA HIDING WITH OPTIMAL VALUE TRANSFER

In reversible data hiding techniques, the values of host data are modified according to some particular rules and the original host content can be perfectly restored after extraction of the hidden data on receiver side. In this paper, the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed.

The secret data, as well as the auxiliary information used for content recovery, are carried by the differences between the original pixel-values and the corresponding values estimated from the neighbors.

Here, the estimation errors are modified according to the optimal value transfer rule.

Also, the host image is divided into a number of pixel subsets and the auxiliary information of a subset is always embedded into the estimation errors in the next subset. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order. This way, a good reversible data hiding performance is achieved.

3.4 SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

This work proposes a novel scheme to reversibly hide data into encrypted grayscale image in a separable manner. During the first phase, the content owner encrypts the image by permuting the pixels using the encryption key. The data hider then hides some data into the encrypted image by histogram modification based data hiding, making use of data hiding key.

At the receiver side, if the receiver has only encryption key, he can generate an image similar to the original one, but cannot read the hidden data. Peak Signal to Noise Ratio (PSNR) of this decrypted image is much higher than the existing methods. If the receiver has only data hiding key, he can extract the data, but cannot read the content of the image.

If the receiver has both keys, he may first extract the data using data hiding key and then decrypt the image using encryption key. The method also has a higher data hiding capacity than the existing reversible data hiding techniques in encrypted image.

3.5 AN IMPROVED REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING SIDE MATCH

This letter proposes an improved version of Zhang's reversible data hiding method in encrypted images. The original work partitions an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels.

The data extraction and image recovery can be achieved by examining the block smoothness. Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction.

This letter adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over Zhang's work. For example, when the block size is set to 8 8, the error rate of the Lena image of the proposed method is 0. 34%, which is significantly lower than 1.21% of Zhang’s work.

IV. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

- **The Watermarked Only Attack (WOA)**
- **The Known Message Attack (KMA)**
- **The Known Original Attack (KOA)**

A. MODULES

4.1 The Watermarked Only Attack (WOA):
In which the attacker only has access to watermarked images.

4.2 The Known Message Attack (KMA):
In which the attack-er has access to several pairs of previously watermarked images and the associated messages. Certainly, the cur-rently transmitted message bits are not known to the attacker.

4.3 The Known Original Attack (KOA):
In which the attacker has access to several pairs of previously watermarked images and the corresponding cover image. Certainly, the current cover image is not known to the attacker.

V. RESEARCH METHODOLOGY

Encryption is the process of converting a plaintext message into cipher text which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers.

The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

OBJECTIVE

In public cloud computing, the clients store their massive data in the remote public cloud servers. Since the stored data is outside of the control of the clients, it entails the security risks in terms of confidentiality, integrity and availability of data and service. Remote data integrity checking is a primitive which can be used to convince the cloud clients that their data are kept intact.

In some special cases, the data owner may be restricted to access the public cloud server, the data owner will delegate the task of data processing and uploading to the third party, for example the proxy. On the other side, the remote data integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on identity-based public cryptography and proxy public key cryptography, we will study ID-PUIC protocol.

MOTIVATION

In public cloud environment, most clients upload their data to *PCS* and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion.

In public cloud, remote data integrity checking is an important security problem. Since the clients' massive data is outside of their control, the clients' data may be corrupted by the malicious cloud server regardless of intentionally or unintentionally. In order to address the novel security problem, some efficient models are presenter.

VI. CONCLUSION

In this paper, we design a secure reversible image data hiding (RIDH) scheme operated over the encrypted domain. We suggest a public key modulation mechanism, which allows us to embed the data via simple XOR operations, without the need of accessing the secret encryption key. At the decoder side, we propose to use a powerful two-class SVM classifier to discriminate encrypted and non-encrypted image patches, enabling us to jointly decode the embedded message and the original image signal perfectly. We also have performed extensive experiments to validate the superior embedding performance of our proposed RIDH method over encrypted domain.

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to all those who provide me the possibility to complete the thesis. I express my sincere thanks to my respected and adored chairman **Mrs.E.Leelavathy Elayappan** and Secretary **Dr.A.K.Ramasamy** for providing support and stimulating environment for developing the thesis work. I am very happy to express my sincere and honorable thanks to **Dr.D.RajaKumari M.Com., M.B.A., M.Phil., Ph.D.,** Principal of our college for her kind encouragement to do this thesis. I would like to express my sincere thanks to **Mrs.C.Renuga M.Sc(CT)., M.Phil.,** HOD Cum Assistant professor, Department of Computer science and their meticulous guidance, teaching and counseling.
I am deeply indebted to my faculty guide **Mrs.C.Tamilselvi M.Sc.,M.Phil.,B.Ed.,** for this unending support and guidance extended and also my gratitude to all other faculty members of the project committee for their guidance provided to me for the successful completion of this thesis. I also thankful to my family members and friends for their moral support in all part of my work. I extent my thanks to Librarian of Bharathiyar Arts and Science College for Women, for their kind help in providing books and journals for the reference work. Last but not least, Once again, I like to thank Almighty for blessing showered on me.

REFERENCES

[1] X. Li, W. Zhang, X. Gui, and B. Yang,"A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Secur, vol. 8, no. 7, pp. 1091-1100, 2013.
[2] C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao,"An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109-1118, 2013.
[3] X. Zhang,"Reversible data hiding with optimal value transfer," IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316-325, 2013.
[4] X. Zhang,"Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 826-832, 2012.
[5] W. Zhang, K. Ma, and N. Yu,"Reversibility improved data hiding in encrypted images," *Sig. Proc.*, vol. 94, no. 1, pp. 118-127, 2014.
[6] M. U. Celik, G. Sharma, A. Tekalp, and E. Saber,"Lossless generalized-lsb data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp.253-266, 2005
[7] M. U. Celik, G. Sharma, and A. M. Tekalp,"Lossless watermarking for image authentication: a new framework and an implementation," IEEE Trans. Image Process., vol. 15, no. 4, pp. 1042-1049, 2006.
[8] Z. Ni, Y. Shi, N. Ansari, and W. Su,"Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006.
[9] W. L. Tai, C. M. Yeh, and C. C. Chang,"Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906-910, 2009.
[10] J. Tian,"Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 2003.

BIOGRAPHY

Mrs.P.SUDHA is presently pursuing M.Phil., Final year the Department of Computer Science and Research from Bharathiyar Arts and Science College (w), Deviyakurichi , Attur (tk),Salem(dt) , Tamil Nadu,India[1].

Mrs.R.Radha M.Sc.,M.Phil.,B.Ed.,Assistant Professor, Department of Computer Science and Research, Bharathiyar Arts and Science College (w), Deviyakurichi , Attur (tk),Salem(dt), Tamil Nadu,India[2].