Review Paper On Digital Steganography In Android Application

Deepak Sharma Anshu Sharma
B-tech Student,Department Of Computer Science And Engineering
ABES Institute Of Technology Ghaziabad,Uttar Pradesh
Gaurav Agarwal
Assistant professor,Department Of Computer Science And Engineering
ABES Institute Of Technology Ghaziabad,Uttar Pradesh

***Abstract*—**

The need of maintaining the secrecy and safety of the data is much more important than the data itself. Digital steganography is the modern weapon that ensures the security of multimedia files . This method comprises of both the cryptography and data hiding technique .

Here in this paper a wide comparison of modern algorithms(DCT,LSB,BIT SLICING)that are used in steganography are discussed considering their past,present,future aspects.

This paper identifies the basic to modern factors that are required to be encountered in today's scenario.

***Keywords*—** *Steganography ,Covered Encryption , LSB,DCT*

INTRODUCTION

The reason why steganography application is reviewed for android is because as on date android is the most popular Operating system. Smart gadgets are so common these days and are used by every person who uses technology in day today life. Also the data needs to be secured more where it is stored in large.On standard scale approximately 85% of the digital data on and off network is accessed through mobile phones,tablets and e-books that runs on the android applications.

Digital steganography technique aims to provide a unrevealed classified communication..This type of technique is also known as data hiding or cover writing.It is till date the utmost method used for maintaining the secrecy of private digital communication[5]. In this the secret file is Encrypted and Implanted in the cover file .The existence of secret file is only revealed to the intended receiver,while other unintended receiver remains unaware of its existence.The encryption of secret file with the secret key is also given as an option to sender for double secrecy.

In steganography ,first the secret file that is to be communicated is chosen then suitable cover file is selected(depending upon file size)then it is encrypted with the private key (in case it is required) and compression of the file is also required in most of the cases thus is given in option, simultaneous to encryption[5].

OBJECTIVE

This paper rolls out the reviews for the results of the efforts made to analyse and compare the various algorithms and techniques used for steganography in android application.

It also attempts to discuss its present problem domain ,possible solution and its future propects .

METHODS

It is well known that android application are user friendly and are commonly used worldwide.Android is one of the major platform to launch a software application because of its large number of users, also even clients or users with less knowledge of technical domain are able to make the most out of it[2].

Methods used in this technique are:-

i) Encryption(optional) -

In order to have double secrecy file is encrypted using a key , into codes depending on the nature of file.

ii) Concealing -

The process of embedding the secret file into the cover file in order to hide it without changing its original content
.

iii) Decryption-
The process of decrypting the file in order to gain the original message using
the key. (It is carried out at receiver's side only in case encryption was initiated at sender's side).

iv) Extraction-
In this process the original file is extracted from stegano file it is done at receiver end[1].

TECHNIQUES

1)There are various techniques used with different algorithm. In order to be the best,the technique has to maintain the following properties.

i) High Imperceptiblity
Ii) High Embedding Strength
Iii) High Robustness
iv) High Invisiblity
v) High Pay Load Capacity
vi) Low Pick Signal Noise Ratio

Imperceptiblity ->
It is the property by virtue of which it is difficult to distinguish between original and stegno-image.

Embedding Strength ->
Size of information that can be concealed without compromising the quality of image.

Robustness -> Strength to withstand failure
.

Peak Signal Noise Ratio(PSNR) -> It is the ratio of difference between the steganofied image and the original image.

Mean Square Error(MSE) -> Result of cumulative squared error between uncompressed and compressed image.

Two categories of techniques used are

1)Spatial Domain Techniques
2)Frequency or Transformation Domain Technique

1) Spatial Domain Technique:-

In it the data is directly hided in the image pixels of cover file.It is a basic and simple technique[7].

Algorithm used-i) LSB
ii) PVD
iii) HSM

i) LSB (Leat Significant Bit) :-

In LSB their are two types of images(of size 8-bit and 24-bit) or cover files are used to perform the embedding operation and the size of the secret message depends upon the cover file,larger the size of the cover file means more amount of secret data can be embedded into the image[7].In this algorithm least significant bit is replad with the information to be hidden.

ii)PVD(Pixel Value Differencing) :-

In this to perform the embedding operation a 256 gray scale image as a cover image is used[7]. In this the image is scanned from the upper left corner and then image is split into number of small blocks and their neighbour pixel divergence or dissimilarity, larger the difference in amount, more secret data can be fixed into the cover file and the secret data is fixed mostly in the edge area because changes of the pixel values are easily noticed by human eyes.

iii)HSM(Histogram Shifting Model) :-

Histogram is a graphical representation which is widely used in the statistic and the mathematics. In which maxima and minima are two value in graph in which the pixel are allocated within this area called histogram and same technique(divide image into blocks) is used[6].

2) Frequency or Transformation Domain Technique

In this the message is hided in significant (suitable)areas in cover file. Which makes it more dynamic and potential against digital image processing operations.

Algorithm used-i) DWT
ii) DCT

i) DCT(Discrete Cosine Transform) :-

It is a frequency domain technique, which is used for the JPEG image format. In this the image transform to frequency domain and image is separated into special sub-bands of frequency with respect to visual qualityThree frequency elements (FL(Largest Frequency), FH(Highest Frequency) and FM(Medium Frequency)) are used in which FM is the region lies between FL and FH and FM is also known as embedding region to provide additional confrontation to lossy compression technique.

ii) DWT(Discrete Wavelet Transform) :-

The discrete wavelet transformation is an implementation of the wavelet transformation using a discrete set of the wavelet scale in other words this transform decomposes the signal into mutually orthogonal set of wavelet The wavelet can be constructed from a scaling function which describes its scaling properties .A wavelet is a localized change of a sound signal in 1-D or localized variations of detail in an image in 2-D.[7]

1-D DWT

In DWT image is represented as a sum of wavelets and for the analysis operation it uses filter bank.when we apply 1-D DWT there are two types of filters((low pass filter,high pass filter) used in which low pass filter gives approximate coefficient and high pass filter gives detail coefficient and then average of fine detail in small area is recorded[8].

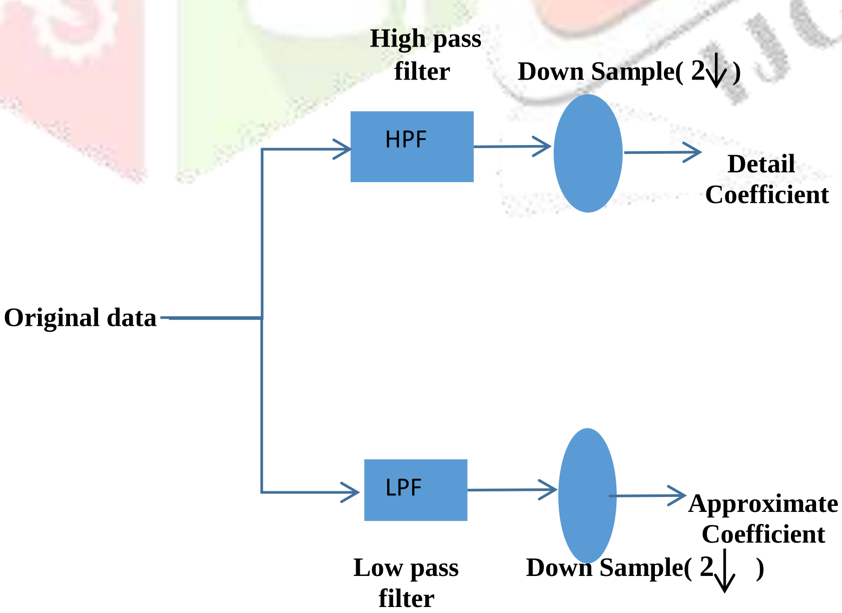

Fig-1D-DWT

2-D DWT

In 2-Dimensional DWT,first we apply 1-D DWT on rows of the image then we apply the same transform to the column of each channel of the result

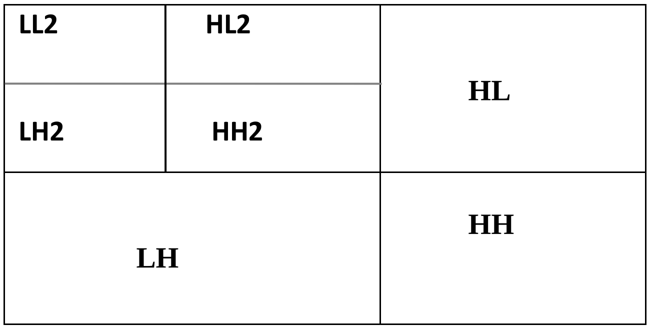

Fig -2D-DWT

For 2-D image representation we can use a 2-D array X[K,L], where K represents number of rows in array and L represents number of column in array and K and L both are the two positive integer. In 2-dimensional DWT firstly we implement 1-dimensional DWT on K(number of rows) and finds the low frequency K and then high frequency L and again 1-Dimensional DWT is performed on column wise and applied on L(number of columns) to find the final coefficient such as LL,HL,LH,HH(Sub-bands) and sub-bands are further decompose into four sub-bands and this process continues to the required number of levels[8].

PROBLEM DOMAIN

The easier it Appears, the Difficult it is. Android is a simple operating system to use but it is much more difficult to built a right product that can work parallel on this platform.Android has its own framework and application programming interface(API), Integrating development environment (IDE), Native application which increases the difficulty to deal with it.The major problems with android mobile phones are.

i) REGULAR UPDATION :-

Android is evolving its own new updated versions ever since it is in use and will continue to update as per present and future requirements. Therefore it becomes all the more necessary to parallely update the steganography application to ensure it continuous use with trend.

ii) INCREASE THE LIMIT ON THE SIZE OF FILE :-

Since amount of data will increase with its use, it becomes necessary to facilitate users by extending the limit of size of files.

iii) LACK OF COMMON VOCABULARY :-

We are well aware of the huge variety of options available in global market (in terms of mobile phone their architecture, system, model and versions etc.)every single feature makes it exponentially difficult to use a common algorithm that is expected to work for every mobile phone and that too with same efficiency.

iv) OPTIONS OF LIMITED OPERATIONS :-

Mobile phones are proven to be the best and the most popular invention of all time.But it is also accepted that it has yet not replaced PC completely its because of its limited applications of operations that it bounds work strength and thus confines only upon certain limit.

v) TESTING ABILITY :-

No matter how smart our phones are, they still fail to provide an environment that can facilitate us to test (run ,compile, develop ,test) our application and program unlike pc.

vi) MANNER OF ACCESSING :-

Approach of accessing the root file in system,depends on the android edition, it is also not commonly known among programmers.

SOLUTION DOMAIN

When their is a will there is a way.Good goals are never easy to achive.Android is not easy to handle but it also has its own advantages.These are

1) It is an open source product.
2) It is based on java, also it has rich sets of application programming interface.
3) It has varied options of integrating development environment(IDE).
4) Android increases its application area (It identifies areas of application like banking, Communication, Storation, Health and Legacy of Services)[3].
5) It is very much in need that we formulate our application on such a algorithm that can give the maximum efficiency withstanding all the covenant and possible future problems.

FUTURE ASPECT

1)With the believe that SAFE FUTURE lies in SAFE DATA, it is undoubted that Steganography will definitely gain trust by increasing its applications and their users. Some other potential research directions are expected to be explore in future like(Application specific,website specific technique specific)

2) Its development with better features with other operating systems(like linux, iOS,blackberry and others)is expected in future[4].

CONCLUSION

1)From our deep study on Digital Steganography in Mobile Application, related articles and research papers it is concluded that Digital Steganography is the best available technique for data safety[4]. Android is as of now the most perfect platform to launch it. (Considering the large number of users that will be benefited out of this).

2)Also There is a need of awaring people that such techniques do exist that are highly efficient in providing data safety by facilitating double secrecy[2].

3)This Application needs to be made handy to increase its accessibility.

4)Regular updation needs to be checked and maintained by authorities or owners to oversee its continuous and satisfactory use.

REFERENCES

[1] Sagar S.Pawar, Prof. Vinit Kakde on "REVIEW ON STEGANOGRAPHY FOR HIDING DATA"international Journal of Computer Science and Mobile Computing ,*April 2014.*

[2] Jibi G Thanikkal1, Mohammad Danish2, Saoud Sarwar on "A New Android Based Steganography Application for Smartphone's"Journal of Basic and Applied Engineering Research,October, 2014.

[3] Parag Himatlal Rughani,Dr. H N Pandya on " Steganography on Android Based SmartPhones",www.ifrsa.org,May 2012.

[4] D. Bucerzan, C. Ratiu, M.J. Manolescu on"SmartSteg: A New Android Based Steganography Application"INT J COMPUT COMMUN, ISSN 1841-9836 ,October, 2013.

[5] Wojciech Mazurczyk and Luca Caviglione on "Steganography in Modern Smart phones and Mitigation Techniques"arXiv:1410.6796v1,27 Aug 2014.

[6] C.P.Sumathi, T.Santanam and G.Umamaheswari on"A Study of Various Steganographic Techniques Used for Information Hiding"International Journal of Computer Science & Engineering Survey (IJCSES),December 2013.

[7] Ramandeep kaur Brar* and Ankit Sharma on"A Review on Steganography "*International Journal of Computer and Information Technology*,*January 2018.*

[8] Akash Goe on"Discrete Wavelet Transform (DWT) with Two Channel Filter Bank and Decoding in Image Texture Analysis"International Journal of Science and Research (IJSR)April 2014.