A High Capacity Crypt-Steganographic Technique Using MD5 Algorithm

Swapnil P. Jahagirdar[1]
*[1](Information Technology,
SNJB's Late KBJ College Of Engineering, Chandwad,
Savitribai Phule Pune University,
India)*

Abstract:-The security of confidential data is very serious problem and challenge for us due to fastest growth in the internet. For this, there are already developed different algorithms and tools to provide the security to the data but then we come to know that this is not enough to provide the security. Steganographic approach hides the data but this also can be attacked by steganalysis. So in this proposed system we combined three technologies for providing ultimate security i.e. cryptography, steganography and hash function. Our idea is to provide ultimate security in securing our data. Message digest of the confidential data is taken firstly and then this hash value is encoded by cryptographic technique and the output message/file can be hide within object, image, video, audio.etc so that the data will secure in efficient way and with more protective way.

Keywords: -Steganography, MD5 algorithm, Capacity.

I. INTRODUCTION

One of the most important factors of information technology is Internet and, communication has very important factorthat is security of information. Cryptography is a technique to ensure the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately sometimes this is not smart enough to keep the contents of a message secure or secret, it may require you to keep the existence of the message secret which ultimately called as Steganography**.**

Cryptography encrypts a message so it cannot be understood; meanwhile Steganography completely hides the message so it cannot be seen. Presently we have very secure methods for both cryptography and Steganography - Even if we combine these techniques as they supposed to be, thereis always possibility that the attacker may detect the original secret message. That's why our idea isto apply them together with more security levels and to get a very highly secure system for data hiding. a new system with extra security features where a meaningful pieceof text message can be hidden by combining the security techniques like Cryptography and Steganography. Steganography methods are classified into spatial domain embedding and frequency domain embedding. Because of low computational complexity and high embedding capacity this project mainly deals with LSB Steganography method. Fig. 1 shows the base embedding technique**.**

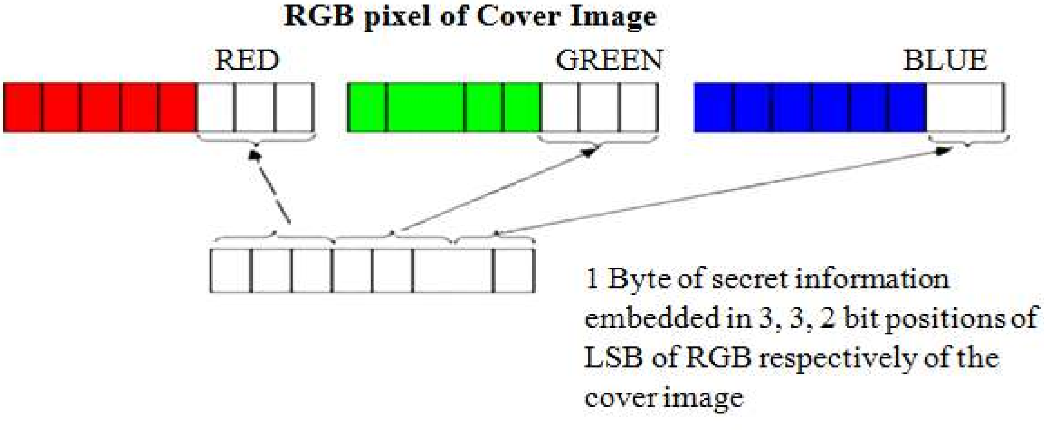
RGB pixel of Cover Image
RED
GREEN
BLUE
1 Byte of secret information embedded in 3, 3, 2 bit positions of LSB of RGB respectively of the cover image

Fig1. Base Embedding Technique (3-3-2 LSB steganography)

The proposed paper contributes enhancement in this above mentioned technique is using the MD5 algorithm and now one should to be able to send any file of any format and of any size which is explained later in the paper. Meanwhile the proposed system will be with the ultimate security and removes drawback of the previous system.

II. RELATED WORK

The current work in providing security also has various techniques and combinations of techniques. Fig 2. Gives idea about the variations of techniques and systems as per there nature. In all previous techniques, there are various Steganographic techniques for various types or kind of information's that we need to send like there are different system to send image or text or audio and videos. And each of them also has drawbacks which are while wants to send an image; the size of image should not be bigger than the cover image. And also there is limitation over how many images that we can send at a time. This all drawbacks are recovered or removed in this proposed system. The current work in our scope of interest area is shown below…

T. Liu and Z. Qiu [1] proposed DWT based color image steganography method. In this method the secret information is embedded into publicly accessed color image by the strategy which is quantization-based. Whereas, the latter case method does the processing overcover object which isgrey scale images for creating subliminal channel. Alsoutilizes transform coefficients of 2-Dimensional Discrete transform for embedding.

Deshpande Neeta et al.[2] proposed the Least Significant Bit (LSB) embedding technique which is suggesting that data could be hidden in the LSB's of the cover image . Meanwhile human eye would not be able to notice the hidden image in the cover file.

Ali Al-Ataby[3] proposed method which is a modified and high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in cover image and also more overall security.

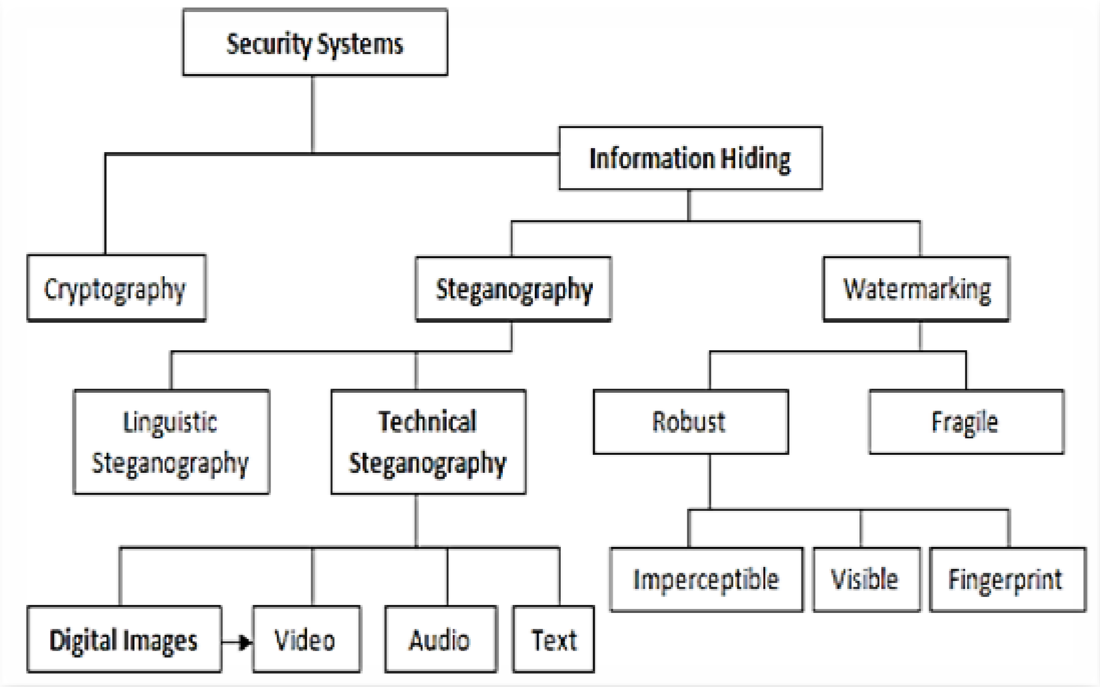

Fig 2. Classification of security system

T. Narasimmalou [4] proposed a new method of image data hiding technique which is based on discrete wavelet transform. Here cover image after the embedding the secret datais looking perfectly intact which in addition has high peak signal/noise ratio value. Hence, an attacker will not be aware of the existence of secret-image. The secret image after extraction is perceptually similar to the original secret image. In this system two different techniques proposed and implemented which are as follows

1. Using three level discrete wavelet transform and
2. Using single level discrete wavelet transform for hiding images.

H.J .Patel et al.[5] have proposed a new variant technique of image steganography which is LSB based. In this, both ends agree on a set of carrier images and some required parameters. Sender then will choose an image which requires least number of bit manipulations on LSB substitution of secret data, and produce stego-image. Receiver after receiving stego-image will extract LSBs along with help of the received parameters. The probability of guessing parameters is very less.

S. Tiwari et al.[6] proposed a modified and a secure image steganographic model via using RSA algorithm and LSB insertion. Firstly, secret data encrypted using RSA public key of recipients. Then after each bit of encrypted message is embedded to the LSBs of image in different images so as to find the best cover image. The cover image which requires minimum number of LSB extract the message in the encrypted form will be the best one which will decryptit using private key.

Stuti Goel et al.[7] proposed the new method for performance and comparison of three base techniques DCT,LSB and DWT is evaluated onthe basis of the parameters MSE, PSNR, Capacity and Robustness. As of the results, it's cleared that PSNR of DCT is high as compared to othertwo techniques. This also implies that DCT ensures best quality of the image. DWT is a very highlyrobust method in which the image is not distort on extracting the message hidden in itand provides maximum security. Theory studies elaborates that the behavior of systems that used to followdeterministic laws but appear random and unpredictable, a dynamical systemthat has a sensitivedependence on its initial conditions; small changes in those conditions can lead to quite different outcomes.

III. METHODOLOGY

The proposed system will combine three different techniques to ensure high security and capacity. The confidential data that we intend to send is referred to as payload. The payload is nothing but the image, text, audio or video etc. file. Firstly the payload is collected in a folder. This file is zipped here andthen the message digest of that zipped fie is calculated so that the size of that folder is compressed and obviously set to a fixed value. Now this processed zip file is encrypted with cryptographic approach and now this encrypted file is ready to embed into the cover image.

System works in THREE stages. First stage is cover image selection and data selection, putit in one folder. Second stage is making zip file of it and apply hash function and find message digest of the zipped file. Third step will be encrypting that file with cryptographic approach. Third and embedding encrypted data in selected cover image and sends it toreceiver. And complete reverse process on receiver side. Fig 3 elaborates the concept and the flow of the proposed system.

Let the system S be represented as

S=Steganographic system
S= I, O, f_s
Where I = $I_1 \cup I_2 \cup I_3 ... \cup I_n$
I is folder which contains set of data that we intend to send.
O is set of outputs
fs is set of functions
O=f_s(I)
fs= $f_{s1} \cup f_{s2} \cup f_{s3} ... \cup f_s n$

Stage 1:-
Cover image selection and data selection, put it in one folder
User manually selects the Cover image (ic) and data to be sent ($I_1 \cup I_2 \cup I_3 ... \cup I_n$). Put
that all data in a folder (I).

If fs1(I) Select cover image then

I= set of data

Stage 2:-
Make zip file of it and apply hash function and find message digest of the zipped file.
The output of 1st stage is the selected cover image and data that is to be send which is now in a folder (I).
Now system will make a zip file (Z) of the I folder.

If f_{s2} (I) find message digest of zip file then
I = zip file, hash function
I = Z+HF
Where I is an encrypted zip file to be send,
HF is a MD5 hash function for calculating message digest or hash value.

Stage 3:-
Encrypting that file with cryptographic approach andembedding encrypted data in selected cover image and then sends.
The output of 2nd stage is a hash value of zip file (I).
Now we have to encrypt the output of previous stage and embed that encrypted zip file into selected cover image (i_C) and now the
Data is ready to send.

If f_{s2}(E) encrypt file then
E= hash value, encryption algorithm
E= I+ CR
Where E is an encrypted zip file,
CR is a cryptographic approach for encryption.

If f_{s2} (O) send file then
O = encrypted zip file, cover image
O= E+ i_C
Where O is an embedded encrypted zip file in cover image.

As we are combining all kind of payload in a folder and providing the security to that folder; drawback of each of the system will reduced upto certain limit. For example now it is easily possible to send the secret image nigger than the cover image size. Also the capacity of number of files can be send at a time is hugely increased just because we are zipping that folder and applying hash function.

MD5 hash function is a hash function which does not have any input size limitation and gives the output of just 128 bits. So the size of the zip file is again drastically compressed into a fix size block.

After the compression of the file we have a compressed file and then the system encrypt this file with some cryptographic approach and then can easily be embedded into the cover image. Due to double compression of the folder the capacity of sending files and size problem and cover image distortion problem can easily be eliminated and also provides the ultimate security.

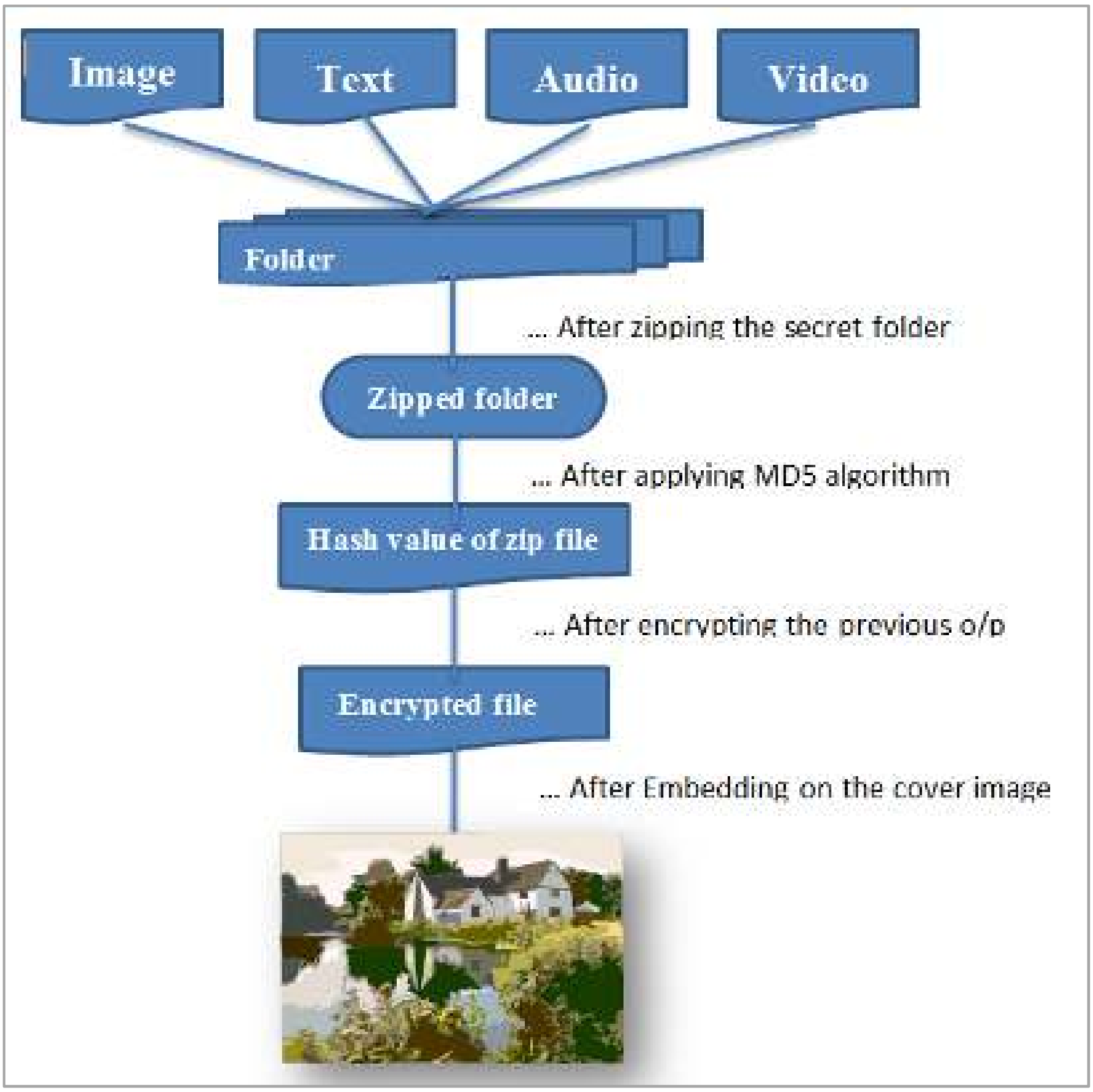
Image
Text
Audio
Video
Folder
... After zipping the secret folder
Zipped folder
... After applying MD5 algorithm
Hash value of zip file
... After encrypting the previous o/p
Encrypted file
... After Embedding on the cover image

Fig 3. Systematic flow of proposed system

The proposed system works on the present system available for secrecy. The first and the most important drawback is; there is separate system for separate type or kind of confidential information the we intend to send over the internet or intranet. In this proposed system we can easily remove this drawback because in this system firstly we are combining all the information, we can say it as payload which might be any kind of data like image, text, audioand video etc.in a folder. As we are going to put all confidential data in a folder now we are able to send any file of any format. So the problem of separation of system due to their type is completely removed.

In previous system, if the secret image that we want to send is bigger in size than the cover image then the cover image is distorted. It is not only possible to remove this drawback but also can be used as an advantage in this proposed system.

The system provides very precious features which are very essential as per the quality andcapacity of the system is concern. The main features of the system are illustrated as,

1. Support of any file format.
2. Support maximum number of files to be send.
3. Provide high security with cryptographic approach.
4. No cover image size limitation.

IV. CONCLUSION

The proposed system combines three distinct techniques hash algorithm, cryptography and steganography which thereby not only boosts security of secret information but also boosts the capacity in huge manner. Hiding and securing enormous data is fully possible. System will not only enhance these aspects but also reduces the limitations of previous system in a huge manner. This type of security is actually needed to stop attacker from attacking the confidential information. And can be used successfully in any area where the security is the most important aspects like government sectors, emails, severs and etc. In the future the systems algorithms can be improved to ensure high security.

V. ACKNOWLEDGEMENT

I would like to thank my project guide Mr. P.R. Bhaladhare, Associate Professor and HOD, Information Technology, SNJB's Late KBJ College of engineering, Chandwad, for his timely suggestions and valuable guidance.

REFERENCES

[1] T. Liu and Z. Qiu, A dwt-based color image steganography scheme, in IEEE, *6th International Conference on Signal Processing, vol. 2, Feb 2002.*

[2] K. S. Deshpande Neeta, Implementationof LSB steganography and its evaluation for various bits, in IEEE, *6th International Conference on Signal Processing i.e. ICSP, Oct 2004.*

[3] Al-Ataby and F. Al-Naima, A modified high capacity image steganography technique based on wavelet transform, in (*IAJIT*)*The International Arab Journal of Information Technology, vol. 7, Feb 2010.*

[4] A. J. R. T. Narasimmalou, Optimized Discrete Wavelet Transform based Steganography,*(ICACCCT)IEEEInternational Conferenceon Advanced CommunicationControland Computing Technology, Oct 2012.*

[5] H. J. Patel and P. K. Dave, Least significant bits based steganography technique,*IJECCE, vol. 3,* pp. 97-103*, 2010.*

[6] P. M. S. Tiwari and N. Shrivastava, The Steganographyanapproach fordatahiding based on encryption and LSB insertion, in *International Journal of Engineering (IJE),Feb 2012.*

[7] M. K. Stuti Goel, Arun Rana, A review of comparison techniques of image steganography,*IOSR-JEEE e-ISSN:2278-1676,p-ISSN:* 2320-3331*, vol. 6, Jun 2013.*