Dual Image Steganography Security and Layers

Bobby.S
Department of Computer Science,
St.Joseph's College of Arts And Science For Women,
Hosur, Tamilnadu, India.

Abstract—Steganography is a process that includes concealing a message in a proper bearer for instance a picture or a sound document. A new encoding scheme is proposed which combines secure data exchange. In this paper presents a novel technique for image steganography and least significant bit(LSB) of each of the pixel's intensity of cover image. In addition with LSB and three layers the secret image is converted into text so that no one can understand the message and then this text embedded in cover image.

Keywords—*Steganography, data exchange, least significant.*

I. INTRODUCTION

Steganography (pronounced STEHG – gruhf- ee, frp, Greek steganos, or covered and graphie, or writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Image steganography methods can be categorized into two parts. One is spatial Domain and other is frequency Domain.

Two types of mechanisms are there to provide security for the information, they are cryptography and steganography. Cryptography means converting the text from readable format to crabbed format. Steganography is used for concealing the information in an image. The information is not visible.

There are three different types steganographic techniques are available for concealing the information in an image, that is Least Significant Bit Insertion, Masking, and Transformation techniques . Least Significant Bit (LSB) embedding is a simple system it implement steganography. The data into the cover so that it cannot be detected by a random observer. The information in a given pixel with information from the data in the image. While it is possible to fix data into an image on any bit-plane, LSB bury is performed on the least significant bits.

Masking and Filtering is a steganography method which can be used on 24 bits per pixel images. The technique can be resort on both color and gray-scale images. Masking and filtering is akin to set watermarks on a printed image.
Transformation use mathematical function to hide least bit co-efficient in the file size of image.

The basic steganography model, the model consists of Carrier (C) , Secret Data (D), and Stego Key (K).
Carrier is the cover object in which the secret message is embedded. Secret data can be any type of confidential data i.e. plain text, cipher text or other image. Key mainly used to ensure that only recipient having the decoding key will able to retrieve the secret message from the cover object. The secret data is embedded in to the cover object in a way that does not change the original image in a human perceptible way. Finally , the stego object which is the output of the process is nothing but the cover object with embedded secret data.

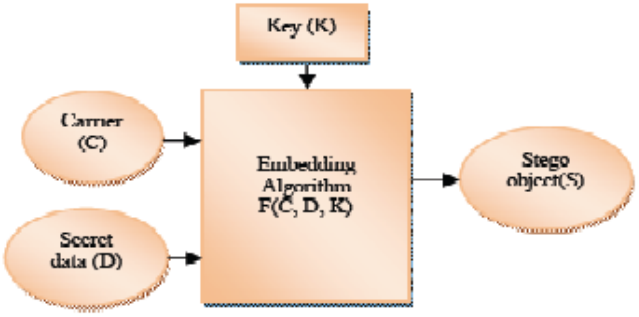

Fig.1. Basic Steganographic Model

II. SECURE DUAL IMAGE STEGANOGRAPHY

The dual image steganography is used the reason behind using image steganography is that images are more popular among the internet users. In this work, 4 bit LSB substitution technique falling under the category of spatial domain is used by which high security is achieved for secret data along with good among of imperceptibility as well as high payload

capacity. Here new version of dual steganography is used where steganography is used within steganography. Here used two process data hiding process and data extraction process .

A. Data Hiding Process:

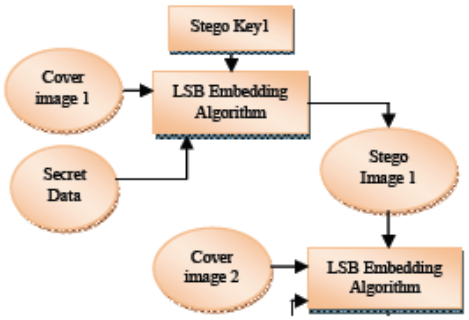

Fig 2.Data Hiding Process

The data hiding technique used two cover images are used i.e cover image1 and cover image2. For providing more security two stego keys are used which are different from each other. The stego key used is of 10 bit in length. The key can be made of numbers, characters and symbols but should be of 10 bit length. These keys are hidden in the cover image during the hiding process. The should be known at the receiver side during the decoding process for retrieving the secret file.

The secret data has been embedded inside the cover image1 with the stego key 1 mainly used for security purpose from which stego image1 is generated and the stego image1 considered as the secret data and hidden inside the cover image 2.

We should using rules.:

- Covr image 1 is separated into RGB planes.

Secret data taken is then converted into binary form.

Those values are separated into upper in two separate planes and lower nibbles which are embedded 4. Upper nibbles are embedded in green plane and lower nibbles in red plane.

- Stego key is embedded in green plane.
- After which, all the three planes are combined to generate stego image1.

Stego image1 is then interpreted as secret data and embedded in the cover image2 using the same thus the final stego image is generated.

B. Data Extraction Process:

The extraction process is process is presented rom the final stego the stego is extract using setgo key1 The data extraction process is presented. Next from stego mage1,secret data is extracted by using stego key2 and same.

We use some steps:

- Final stego image is separated into RGB planes.
- Stego key which acts as password in entered which is then verified with the stored key that is embedded in the blue plane of cover image2.
- If the key is matched then the upper and lower nibbles of binary secure data is extracted from green and red planes respectively.
- Then the upper and lower nibbles and combined to make the binary from of stego image1.
- Finally the original stego image1 is obtained from binary form.
- Next, using the same the original secret data is retrieved from stego image1

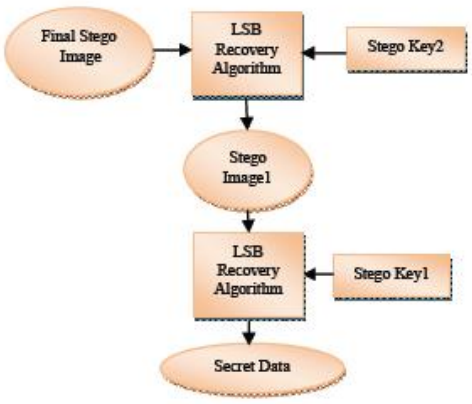

Fig 3.Data Extraction Processes

The extraction process is strictly as the secret data is extracted from stego without the original cover image without the original cover image reference. The complete and successful extraction of data needs the

knowledge of keys k1 and k2 which been extracted from blue plane of cover image. To make the secret data extraction more cumbersome the concept of hiding the secret data in two planes has been adopted.

The image steganography is proposed and the block diagram .

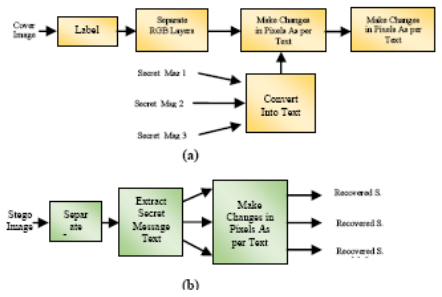

Fig 4.A.Secret Message Embedding Processes
B. Secret Message Embedding Processes.

III LAYERS OF IMAGE STEGNOGRAPHY

Steganography is the invisible communication. The goal of steganography is to secure communication. The general idea of hiding messages in common digital contents, interests a wider class of applications that go beyond steganography. The methods involved in such applications are collectively referred to as information hiding.
For example, while it is possible to add metadata about an image in special tags (exif in JPEG standard) or file headers, this information would be lost when the image is printed, because metadata inserted in tags on headers are tied to the image only as long as the image exists in digital form and are lost as soon as the image is printed. By using information hiding methods, it is possible to fuse the digital content within the image signal regardless of the file format and the status of the image (digital or
analog). Moreover, we will refer to the secret message as stego-message or hidden message. Depending on the meaning and goal of the embedded metadata, various information hiding fields can be defined, even though in literature the term „information hiding" is often used as a synonym for steganography. In the digital watermarking,
for instance, the information is used for copy prevention, copy control, and copyright protection. In that case the embedded data should be robust to malicious attacks in order to preserve its goal.
The key difference between steganography and watermarking is the absence (in steganography) of an active adversary mainly because usually no value is associated with the act of removing the information hidden in the host content. Nevertheless, steganography may need to be robust against accidental or common distortion like compressions or color adjustment (in this case we will talk about active steganography). On the other side, steganography wish to communicate in a completely undetectable manner which does not need to
be required in watermarking. For this reason we can consider steganography also as part of cover communication science.

IV DUAL STEGANOGRAPHY APPROACH FOR SECURE DATA

The The late development in computational force and innovation has pushed the requirement for exceptionally secured information correspondence. One of the best strategies for secure correspondence is Steganography-an undercover composition. It is a specialty of concealing the very presence of imparted message itself. The methodology of utilizing steganography as a part of conjunction with cryptography, called as Dual Steganography, builds up a strong model which includes a great deal of difficulties in recognizing any concealed and
scrambled information. Utilizing cryptographic systems to scramble information before transmission may prevent any sort of security issues. Be that as it may the disguised appearance of scrambled information may stimulate suspicion. Along these lines utilizing steganography inside steganography, offer climb to enhanced form of double steganography which will give better security.

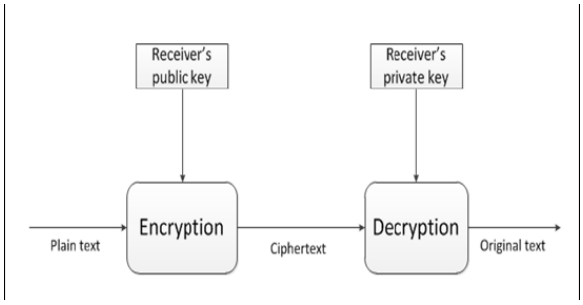

Fig 5.Cryptography flow

Steganography is the investigation of undetectable correspondence which shrouds any private information inside a blameless looking spread item. The statement Steganography is gotten from the Greek words "stegos" signifying "spread" and "grafia" signifying "composition" characterizing it as "secured written work" .Steganography is not quite the same as cryptography. The objective of ptography is to give secure interchanges by changing
a third individual to figure out the message. Not at all like steganography, sending scrambled data may draw consideration. Steganography today, then again, is altogether more complex, permitting a client to conceal a lot of data inside picture and sound documents.

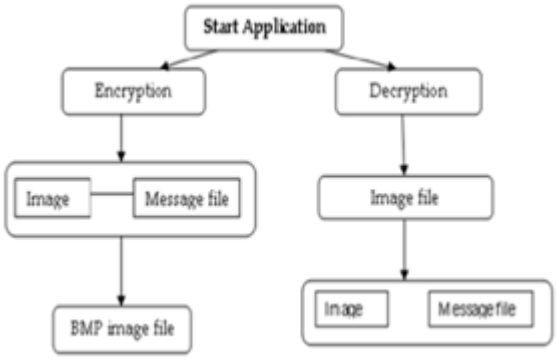

Fig 6.Steganaography flow

CONCLUSION

Data security has turned into a standout amongst the most huge issues because of the exponential development of web clients. Unapproved access to mystery information can have genuine repercussions like monetary misfortune and so on. Steganography is one of the arrangements whose objective is to conceal the presence of imparted message. In
this paper, exceedingly secured information concealing strategy has been exhibited where steganography is utilized inside steganography. The proposed strategy implants information in two spread pictures utilizing Six bit LSB method. The mystery information is covered up in double structure in two spread pictures because of which twofold insurance has been given to classified information which
can be any content, sound, feature or picture. The trial results demonstrate that the proposed plan can be a decent option for secure correspondence where two level of security is acquired in conjunction with high payload limit and great subtlety.

FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in the future. Such as with the help of pre-emptive approach more information can be added for exact, timely analysis with high accuracy. It can also be used for quantitative & qualitative analysis, rank ordering, etc. We also embed the source code of our proposed scheme in Java. In our proposed scheme so as to use the benefits of an approach like open source.

REFERENCES

[1]Sujay Narayana and Gaurav *Prasad "Two new approaches for secured image steganography using cryptographic techniques and type conversions"* , An International Journal(SIPIJ) Vol.1, No.2, December 2010
[2] Clair, Bryan, *"Steganography: How to Send a Secret Message",8-* Nov.-2001 www.strangehorizons.com/2001/20011008/steganography.shtml.
[3]Moller. S.A., Pitzmann, and I. Stirand, "*Computer Based Steganography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best*", in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer,1996,pp.7-21.
[4]Gruhl, D., A. Lu, and W. Bender, "*Echo Hiding in InformationHiding*", First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer,1996,pp.295-316.
[5]Kurak, C., and J. McHughes, "*A Cautionary Note On Image Downgrading*", in IEEE Computer Security Applications Conference 1992, Proceedings, IEEE Press, 1992,pp.153-159.
[6]van Schyndel, R. G., A. Tirkel, and C. F. Osborne, "A *Digital Watermark*", in Proceedings of the IEEE International Conference on Image Processing, vol. 2, 1994, pp. 86-90.
[7]Johnson, N. F., and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, vol. 31, no. 2, 1998, pp. 26-34.
[8]Rhodas, G. B., "*Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image*", U.S. Patent5,710,834,-1998.

[9]Swanson, M. D., B. Zhu, and A. H. Tewk, "*Transparent Robust Image Watermarking*", in Proceedings of the IEEE International Conference on Image Processing, vol. 3, 1996, pp.211-214.
[10]Pitas, I., "*A Method for Signature Casting on Digital Images*," in International Conference on Image Processing, vol.3,IEEEPress, 1996,pp.215-218.
[11]Maxemchuk, N. F., "*Electronic Document Distribution*", AT&T Technical Journal, September/October 1994, pp.73-80.
[12]Low, S. H., et al., "*Document Marking and Identifications Using Both Line and Word Shifting*," in Proceedings of Infocom'95,1995,pp.853-860.
[13]Low, S. H., N. F. Maxemchuk, and A. M. Lapone, "*Document Identification for Copyright Protection Using Centroid Detection*", IEEE Transactions on Communications, vol. 46, no. 3, 1998, pp. 372-383.
[14] Kirti Shukla et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1632-1635, www.ijcsit.com 1635