ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Hybrid Fusion Methods in Image Steganography for Secured Data Transmission

Usha B.A[1], Dr.N.K Srinath[2], Dr. Ravikumar C N[3], Puttaraju[4], Manu[5] & Vijaykumar[6]

Assistant Professor, Department of CSE, R.V.C.E, Bangalore[1]

Professor and Dean PG Studies, Department of CSE, R.V.C.E, Bangalore[2]

Professor and Head, Department of CSE, SJCE, Mysore[3]

Final Year BE, Department of CSE, R.V.C.E, Bangalore[4,5,6]

Abstract: In the present digital scenario, safe and protected communication is the most important requirement. Steganography is the process of implanting secret information into a multimedia carrier it may be text, image, video or audio etc., by hiding information in the image such a way that no one apart from the intended recipient knows of the occurrence of the message. Image fusion is the operation of mixing relevant information from two or more pictures into a single image. In this paper, the Steganography and the image fusion processes are distinct. By the combination of both processes, the security will be more and it tends to new emerging technology. By applying hybrid fusion where the images are fused twice using an effective fusion method that provides enhanced resultant image. The project Hybrid fusion method in image Steganography finds an application in a very wide range of areas involving image processing.

Keywords: Image steganography, DWT, PCA, Image fusion, Hybrid Fusion.

1. INTRODUCTION

Steganography is the art and science writing or hiding the message that communication is taking place, by hiding information in a image such a way that no one apart from the intended recipient knows of the existence of the message. Hybrid Fusion is the process of combining relevant information from two or more images into a single image. Image fusion methods can be broadly classified into two groups Spatial domain [1] and Transform domain fusion. In spatial domain images fusion were the pixels values are directly manipulated to achieve desired result. In Transform domain fusion images are first transferred in to frequency domain, after that fusion operations are performed on the image. Use of the Simple primitive technique will not recover good fused image in terms of performance parameter like peak signal to noise ratio, Normalized correlation, and Men square error. Combination of Discrete Wavelet Transform and Principal Component Analysis [2], have been popular fusion technique. These methods are used to perform much better image quality.

Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication [3] that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication [4][5] is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stego-image (generated image which is carrying a hidden message). The term fusion means in general an approach to extraction of information acquired in several domains. The goal of image fusion (IF) is to integrate complementary multisensor, multitemporal and/or multiview[6] information into one new image containing information the quality of which cannot be achieved otherwise. The term quality, its meaning and measurement depend on the particular application. Image fusion [7] has been used in many application areas. Numerous fusion applications have appeared in medical imaging like simultaneous evaluation of CT, MRI, and/or PET images [8]. Plenty of applications which use multisensor fusion of visible and infrared images have appeared in military, security, and surveillance areas. In the case of multiview fusion, a set of images of the same scene taken by the same sensor but from different viewpoints is fused to obtain an image with higher resolution than the sensor normally provides or to recover the 3D representation of the scene. The multitemporal [9] approach recognizes two different aims. Images of the same scene are acquired at different times either to find and evaluate changes in the scene or to obtain a less degraded image of the scene.

Any piece of information makes sense only when it is able to convey the content across. The clarity of information is important. Image Fusion [10] is a mechanism to improve the quality of information from a set of images. By the process of image fusion the good information from each of the given images is fused together to form a resultant image whose quality is superior to any of the input images. This is achieved by applying a sequence of operators on the images that would make the good information in each of the image prominent. The resultant image is formed by combining such magnified information from the input images into a single image.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

1.1 Methodology

The methodology used while embedding is least significant bit i.e. the eighth bit inside an image is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components, since they are each represented by a byte. An 800×600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. Standard Image Steganography algorithm to hide secret data in the image. At the sender side, secret data is embedded and the resulting images are fused together by using DWT (Discrete wavelet Transform) and PCA (Principle component analysis) image fusion techniques. At the receiver end defusion and extraction takes place. Matlab and its API's are used to implement the steganography and fusion technique.

2. HYBRID FUSION METHOD IN IMAGE STEGANOGRAPHY

The Hybrid Fusion technique involves Fusion of images at the sender side and de-fusion at the receiver side. Before the Fusion process of images, the Steganography is applied to the cover images and extraction is applied at the receiver end after the defusing process of image. Hence the Fusion technique adopts the concepts of image processing as the target scope.

2.1 Image processing

Image processing is a technique to change an image into digital form and perform certain operations on it, in order to get an improved image or to extort some helpful information from it. It is a kind of signal dispensation wherein input is image and output may be picture or characteristics associated with so as to image. Typically **Image processing** system incorporates treating images as 2 dimensional signals as submitting already set signal processing method to them.

2.2 Steganography

Steganography is the art and science of writing or hiding the message that communication is taking place, by hiding information in a image such a way that no one apart from the intended recipient knows of the existence of the message. Image Steganography is referred as taking the cover object as image in Steganography [17]. Typically, in this method pixel sharpness are used to conceal the information. In image Steganography nearly all data concealing methods try to change unimportant information in the wrap image. Least significant bit (LSB) [18] incorporation is a usual, easy approach to implanting the information in a wrap image.

2.3 Fusion

Image Fusion is the process by which two or more pictures are mixed into a single image keeping the significant features from each of the original pictures. The fusion of pictures is often needed for images obtained from dissimilar instrument modalities or capture methods of the similar sight or objects. Fusion methods contain the easiest method of pixel averaging to more complicated techniques like principal component analysis and wavelet transform fusion. Various methods to image fusion can be differentiated, depending on whether the pictures are combined in the spatial domain or they are changed into another domain, and their transforms are mixed.

PCA is a mathematical tool which transforms a number of correlated variables into a number of uncorrelated variables. The PCA [19][20] is used extensively in image compression and image classification. The PCA involves a mathematical procedure that transforms a number of correlated variables into a number of uncorrelated variables called principal components. It computes a compact and optimal description of the data set.

2.4 Defusion

Image Defusion is performed to retrieve the original images from fused images. The defusion is the inverse process of fusion. The inverse discrete wavelet transform is applied to get the original images from fused image. After the defusing of images inverse Steganography is needs to be applied to get the secret data.

3. IMPLEMENTATION

A method of realization of a technical specification or algorithm as a program, software component or other computer system is basically called as Implementation. The low level design details are converted into a language specific program such that they satisfy the requirements of the given software. The technique used for implementing the software must support reusability, ease of maintenance and should be well documented. The choice of languages and platform for implementation also plays a very important role. The implementation phase should follow a well-structured approach which is based on popular software engineering practices.

The most important phase for any project development is implementation since it yields the final solution, which solves the problem at hand. The implementation phase involves the actual materialization of the ideas, which are expressed in the analysis document and developed in the design phase. Implementation should be a perfect mapping of the design document in a suitable programming language in order to achieve the necessary final product. Often the product is ruined due to incorrect language choice for implementation or an unsuitable method for programming. In the following section factors about the programming language and platform selection are described.

3.1 Platform

As previously stated, the programming language selected should have reflection of requirements of the project to be completed expressed in terms of analysis and design documents. Some of the features that are required are stated below:

- Signal processing is an important necessity in the project as preprocessing module heavily requires processing of input signals.
- Matrix manipulations are another important requirement. A language, which provides quick and easy implementation for matrices are preferred as

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

computationally heavy and matrix manipulations are necessary.

- Considering the present emphasis on graphical user interface, the language must have tools to create pleasant looking and simple to use user interface. Linking the front end with the backend code should be also easy.
- Other than the above specific requirements few general requirements like the language should be simple to learn and code, should provide debugging features etc., and should make a contribution towards deciding the language of implementation.
- All these requirements are supported in MATLAB.

4. EXPERIMENTAL RESULTS AND ANALYSIS

Image Fusion system is developed to embed the secrete data into the cover images, then fuse the two stego image by applying image fusion technique called DWT(Discrete Wavelet Transform) and PCA(Principle Component Analysis) where the image fuse twice all these process is done at sender side. In order to get the original secrete data at the receiver end first defuse the fused image using IDWT image fusion technique and inverse stego for extracting the original secrete data from the cover image. Finally it will compare the results to ensure that recipient receive the correct secrete data.

4.1 Experimental Dataset

The dataset on which the experiment was conducted on more than 15 cover images. Example of cover image size 606Kb and dimension 1024*768, secrete data of the size 400Kb and over image of size 759Kb and dimension 1024*768, secrete data of the size 600Kb. The input parameter list for the operation was given through a GUI push buttons in MatLab 2009. Each time cover image and secrete data is loaded using the GUI button in both at the sender and receiver end.

4.2 Performance Analysis

When the image undergoes fusing twice and embedding o the secrete data in an efficient way to ensure that confidentiality and integrity of the secret data. The sender can send two stego images by fused into singe image, so it reduces the traffic of network.

The system is accept the secrete data as input. Then the secrete data is embedded in the cover images, same thing is repeated for another cover image then fed into fusion process to fusing the image and then send that stego-fused image over a network. At the receiver end don't bother about cover image but ensure that receiver should receive the correct secrete data which is send by the sender. Image quality is measured by using the parameter called MSE and PSNR which is shown in Figure 4.1.

In Figure 4.2, the name above illustrates the PSNR (Peak signal to Noise Ratio) for different resolution images. PSNR value will defends on size of the secrete data embedded in the cover image as well as resolution of the stego image.

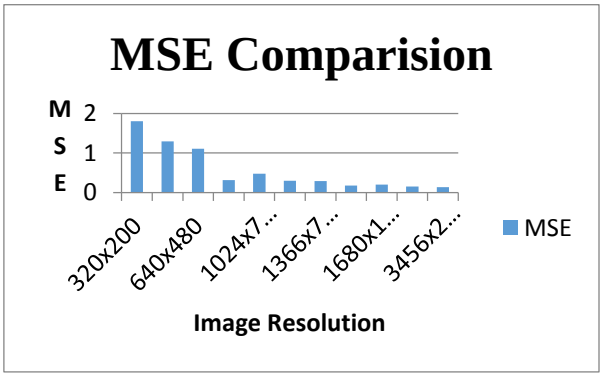

Figure 4.1: Mean square Error for different resolution of Stego images with respect to secret data size

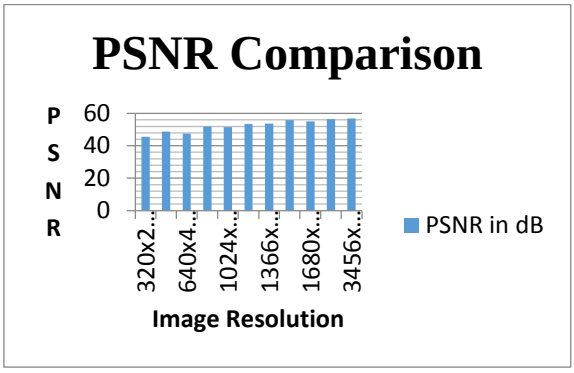

Figure 4.2: PSNR Comparison for different Resolution of Stego Images

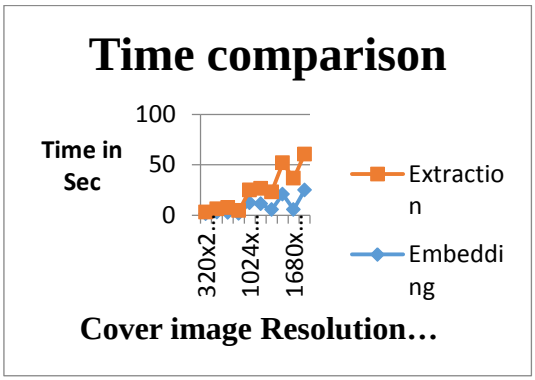

Figure 4.3: Time comparison for embedding and extraction of secrete data

The Figure 4.3 shows the time comparison of the Embedding and Extraction process means time taken to embed the secret data at sender side and extract that secret data at receiver end.

In Figure 8.4, the name below the highlighted portion of Steganography embedding process. The result of the same method produce a stego image which consist both secrete data and cover image. stego image is given as input to fusion module, here fusing of two image is done by DWT and PCA image fusion method. Figure 8.5 shows the user interface of complete image fusion system of both sender and receiver end.

4.3 Inference from the Result

It is clear from the experiment result that the same secrete data is arrives at the receiver end without any modification by the unintended person. The image fusion

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

system has reduced the network traffic and provide the two level of security and hybrid fusion method ensure the quality of input secrete image after arrives at the receiver end.

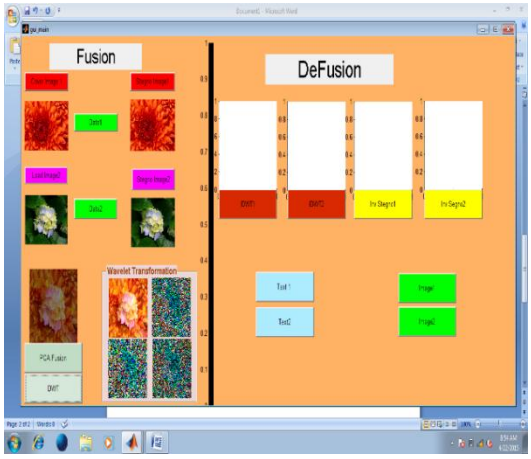

Figure 8.4 Complete image Fusion System

Figure 8.5: Complete image DeFusion System

5. CONCLUSION

Hybrid Fusion Method in Image Steganography is an efficient way of hiding Secret data in an image for secured data transmission. By using this application any text files and image files could be transmitted to intended recipient. If the hacker tries to gather the secret data, they will be failed to access the proper secret data, because they needs to defuse the image first.

When the PCA fusion process applied to images, the Peak Signal to Noise Ratio (PSNR) values of the images is 76.44 dB, but it may produce Spectral degradation. Our project is combination of the PCA and DWT fusion method which achieves the PSNR values are approximately 56 dB and high spatial resolution with high quality spectral content.

The Hybrid Fusion Method in Image Steganography provides two level security. First one is Steganography and the second one is fusion of stego images. If the Man in the middle attack occurs, the hackers are needs to be defusing the image first and then apply the inverse steganography. Otherwise the secret data will not be revealed. If the unintended user get to know about fused images and tries to defuse it, they have to use IDWT technique only. Otherwise the proper images will not be the output. If the hackers get succeeded to defuse the image by using brute force attack, they are not aware of Steganography after the defusion. Their thought might be the just sending of two images simultaneously by combining both, instead of sending individually.

5.1 Future Enhancement

In the future enhancement, the size of the secret data can be more than the size of cover image. The all formats of text files can be hided in the cover image in future, this is needs to implement. The encryption of secret data can also be done before the hiding of data in an image. This could increase the security level of transmission. The fusing of more than two images can be implemented in future. And more than two fusion techniques can also use to fuse the images. The better algorithms can be used to hide the secret data in future. This will provide robust security against the unintended user. In future try to improve the other parameters such as PSNR of images by using other fusion techniques to maintain the quality and resolution of images.

REFERENCES

[1] Sehasnainjot Singh, "Literature survey on Image Fusion Techniques", An International Journal of Engineering Sciences, Issue, Vol. 2, December 2014, pp. 40-43

[2] NamithaTiwari, Dr. MadhuSandilya, Dr. MeenuChawla, "Spatial Domain Image Steganography based on Security and Randomization", International Journal of Advanced Computer Science and Application, Vol.5, No. 1, 2014, pp.156-159

[3] GazaMalhotra, Dr. Vinay Chopra, "A Review on Various Image Fusion Techniques", International Journal of Computer Engineering and Applications, Volume VI, Issue III, June 2014, pp.49-59

[4] G ArunKarthick, K. Kavitha, V.Sivakumar, D Surender, "A Hybrid Method for Covert Communication using Steganography and Image Fusion", International Journal of Advances in Engineering & Technology, ISSN. 22311963, May, 2014. pp. 35-43

[5] Aradhana Sharma, Ahmed Mohammed, " Three Level Wavelet Decomposition Hybrid Transform Image Steganography", International Journal of Advanced Electronics & Communication systems, ISSN NO. 2277-7318 ISSUE 2 VOL 3, APR-MAY-2014, pp. 62-68

[6] Sonali Mane, S. D. Sawant, "Image Fusion of CT/MRI using DWT,PCA Methods and Analog DSP Processor",Sonali Mane et al Int. Journal of Engineering Research and Applications, ISSN.2248-9622, Vol. 4, Issue 2February 2014, pp.557-563

[7] Hongyuan Jing and Tanya Vladimirova,"Novel PCA Based Pixel-Level Multi-Focus Image Fusion Algorithm", NASA/ESA Conference on Adaptive Hardware and Systems (AHS) 2014, pp. 56-62

[8] Sweta K. Shah, Prof. D.U. Shah, "Comparative Study of Image Fusion Techniques based on Spatial and Transform Domain", International Journal of Innovative Research in Science, Engineering and Technology, ISSN. 2319-8753, Vol. 3, Issue 3, March 2014, pp.10168-10175

[9] Sonia Kuruvilla, J. Anitha, "Comparison of Registered Multimodal Medical Image fusion Techniques", International Conference on Electronics and Communication System (ICECS -2014), pp. 124-128.

[10] RakeshAdityaMitraHirve, "A Comparative Analysis of Wavelet Transform & PCA Image Fusion Techniques"| Volume 2, Issue 2 | ISSN. 2321-9939, 2014, pp. 2437-2441