A HYBRID METHOD FOR COVERT COMMUNICATION USING STEGANOGRAPHY AND IMAGE FUSION

[1]G. Arun Karthick, [2]K. Kavitha, [2]V. Sivakumar, [3]D. Surender
[1]Department of Embedded System and Technologies
[2]ACTS, Centre for Development of Advanced Computing (C-DAC), Pune
[2]SS & DM Group, Centre for Development of Advanced Computing (C-DAC), Pune
[3]Assistant Professor, Department of EEE
[1,3]Veltech DR.RR & DR.SR Technical University, Avadi

ABSTRACT

Day to day, network and its technologies is getting rapid growth, due to its improved infrastructure in to hold on; the situation organization and migration of recent updates will leads the network called Security flaw. Various security options are available since the data leakage and back door communication leads to heavy data loss to the organization. In this paper we developed a new scheme which is hybrid in nature, combines two distinct domains. 1) Steganography (Combination of Image + cryptography) and 2) Image Fusion – Fusing two images. Steganography embeds the digital data message along with the media file where digital data may be text, image or hybrid. Although both Cryptography and steganography are combined to provide security in some criteria yet advanced system of security is needed to share information without any interference. To overcome the real world problem we proposed a novel algorithm called StegFuse where cryptography and steganography is applied on two various images, after applying steganographic technique both the images are subjected to image fusion in order to get the fused image. Wavelet transform is applied on both the image during fusion. Traditional cryptographic techniques are used for encryption of digital data and steganographic algorithms are used to hide the encrypted data in the images.

KEYWORDS–*Steganography; Image Fusion; Encryption; Decryption; Public Key; Private Key*

I. INTRODUCTION

Tremendous growth in networks leads to data/information sharing. Though the security level of these technologies was high, still there is third party interference to deal with other’s data and hijacking the information. Many cryptographic techniques were proposed by various researchers.

Basics about Cryptography

Symmetric key Cipher-In this technique both the sender and receiver uses common key for encryption and decryption [1-5]. Symmetric key technique is faster, the main flaw is both the sender and receiver has to transfer the key in secured way. Most common and popular example of this type of technique is Data Encryption Standard (DES) [1-5].This is also known as secret key Cryptographic technique. Asymmetric key Cipher-In this technique both sender and receiver uses different key for encryption and decryption. A Public key (Asymmetric key) used for encryption and a secret key used for decryption. Here public key is distributed insecure way and secret key is never transmitted [2]. Here this technique is slower but highly secured. Hybrid Cryptographic system-Hybrid cryptographic system uses both the public and secret key cryptographic techniques. This technique attains more complex when compared to other techniques [14].

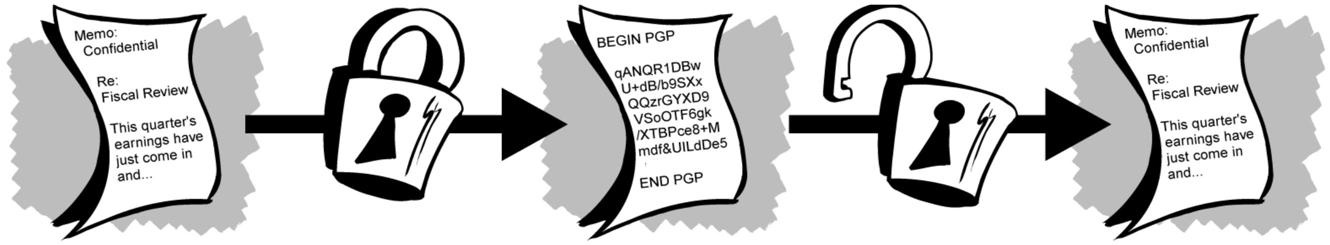


Figure 1: Steganography work flow [figure adapted from 1]

Basics about Steganography

Steganography [6][3][7] are encryption standard which ensures to confidentiality of data's. In encryption the main drawback scenario is anybody can see the secret communication channel (message passing) but it is quite complicated to retrieve the encrypted data but in Steganography, it hides the information where the communication channel is invisible so that no one can know about the information/message sharing [9]. It provides a secret communication channel which cannot be removed or retrieved without altering the embed information or data [15]. The most commonly used steganographic technique was bit insertion method where the least significant Bit (LSB) of the pixel is modified and projected [1].The Steganography methodology used in this paper was modified bit encoding method in which each pixel can store/hold 8bit of data [3][13].

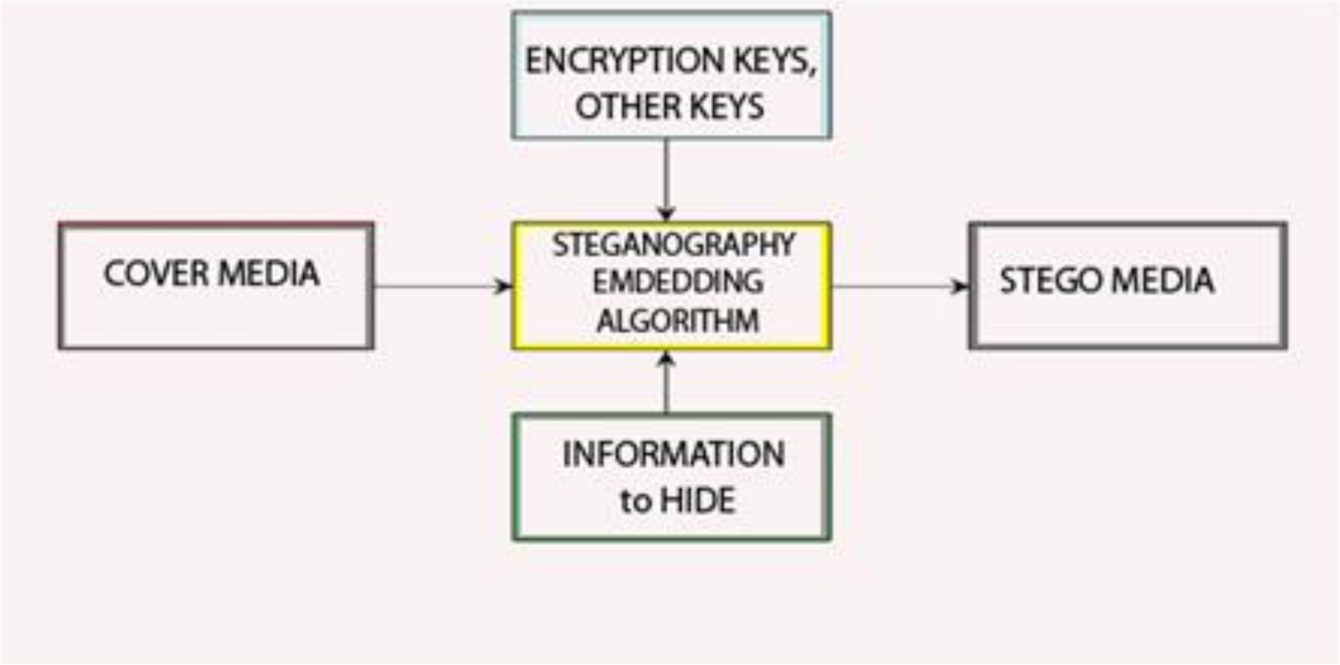


Figure 2: Basic work flow of Steganogrpahy

Basics about Image Fusion

Image fusion is merging two different images in order to retrieve more information from the images. Fusion is applied for the partial distorted images and it is fused in order to retrieve necessary information from fused image. It is applied in normal JPEG image frames which is similar to each other (i.e., frame after other).

II. Proposed Methodology

In general Cryptographic algorithm needs reference table in order to convert small block of data into another block of data. In order to provide high end security, reference table is indexed with reference database which it contains various 3D data grids; datasets are of 3d in order to represent each character in data grids as numbers. Initially the two distorted images and distorted coefficient are mapped in the images using correlation coefficient values from the separate matrix [12]. Data value with similar pixel co efficient is considered to be distorted region.

$$Co_{xx} = \frac{\Sigma_p \Sigma_q \left(U_{pq} - \frac{1}{U}\right)\left(V_{pq} - \frac{1}{V}\right)}{\sqrt{[\Sigma_p \Sigma_q \left(U_{pq} - \frac{1}{U}\right)] \cdot \Sigma_p \Sigma_q \left(U_{pq} - \frac{1}{U}\right)] \cdot [\Sigma_p \Sigma_q \left(V_{pq} - \frac{1}{V}\right)] \cdot \left(V_{pq} - \frac{1}{V}\right)]}} \text{ --------------- [1]}$$

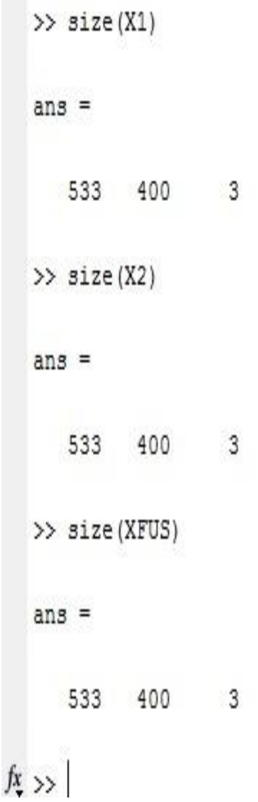
Asymmetric key cryptographic Technique [2] is applied for encryption of data along with the key. Generate Cipher and now cipher is included (hidden)in the single image file where another image file is simply at rest; using modified bit encoding algorithm which prune the pixel value with nearest zero and number in datasets(reference grid)will be included for the appropriate character. Each and every character in the message text will acquire an initial change in the RGB values. Basically initial change should be >5.The change made will be unique for each character. For every 8 bit in the pixel, 1 bit is edited for the message character (number according to reference grid (reference table)).In this technique the general attributes of the images will be encrypted and saved so that it can provide necessary information even though the image format is changed from one format to another (say JPEG to GIF, JPEG to PNG, JPEG to TIFF) etc. This encrypted attributes information is used for decryption purposes [2]. The general attribute information from two images is taken and a key factor value is assigned to it. To decode the information from the image key factor value should be known. Now both the images are subjected to fusion technique. Here we apply general Curvelet [4] transform for obtaining multi high resolution images. Curvelet [4] co-efficient are mapped for both the images. Based on fusion rules, pixel based rule is applied for fusing two images, window based rule is applied for correlating the key factor value of both the images. Now the fused Curvelet coefficients are taken and mapped with the fused images. Distorted image can be reconstructed as normal image using fusion technique. Fig 2 shows the implementation result of fused images[16]. Decryption is done using reversible method where the normal image holds the key factor value and it is fused with the distorted image. Hence fused image is sent to receiver side, where the receiver gets the key factor value from the fused image(normal image) and can retrieve the message or data from the fused image(distorted image).

III. ALGORITHM

```
Begin
Function [C,K,XFUS] = StegFuse[Cipher,Img1,Img2,Key,Message]
Input=image1,image2,Cipher_key,Message
Output = Cipher_Text(C),Key_Factor,Fused_Image
For i=2:
Get(img1,img2);
End for
Get(Key,message);
Encrypt(DEA,&key,&message);
Disp(Cipher,encrypt());
Foreachpixel_val>0; pixel_intensity<5;
R=03;B=04;G=04;
Steganography(&img1,&img2,Cipher,encrypt());
Curvelet (steganography());Reconstruct(Img1,Img2);
ImgFus(curvelet(),Reconstruct());
Disp(ImgFus());
```

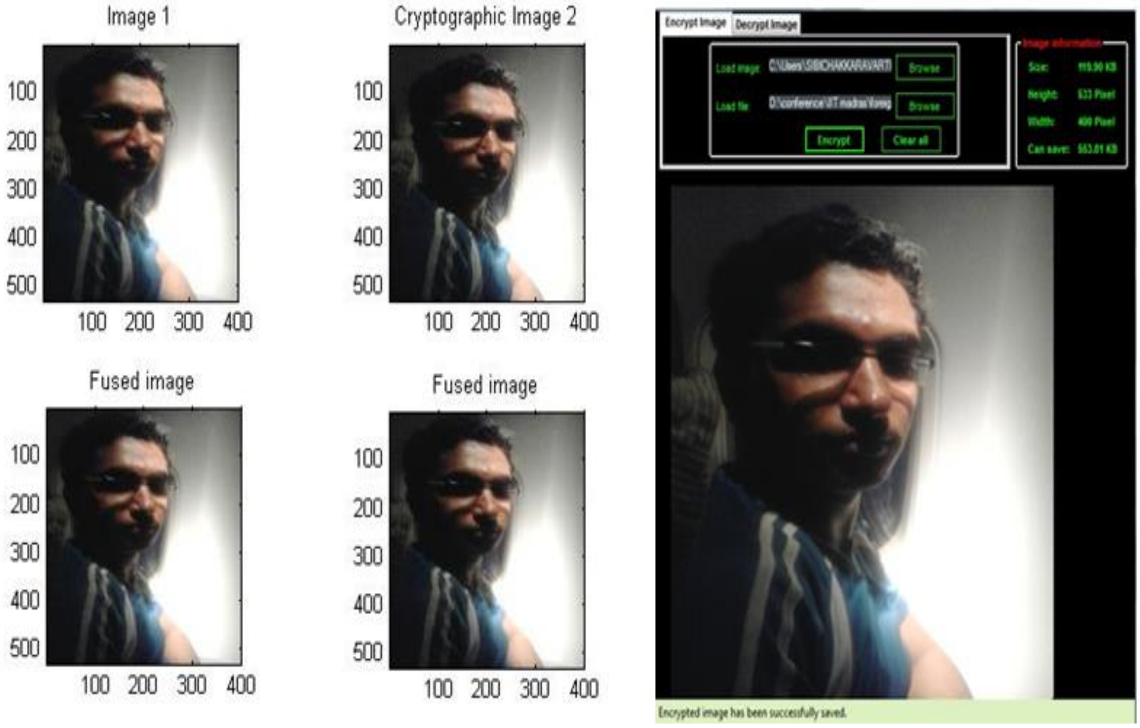
IV. IMPLEMENTATION RESULTS

The technique was developed using the images of same size 400 x 563. The key text was “hi I am G.Arun Karthick”, the message was encrypted into cipher text and the encrypted cipher was implanted to the image using modified bit encoding [2] method by pruning the nearby pixel value to zero where the pixel are represented using colourmap-JET. The reference db is selected based on pixel values i.e., by means pixel intensity. Image which contains message does acquire any loss in their general form. Figure 2& 3 shows the experimental results of StegFuse Technique. Each image is of size 533 x 400 3 for Red, Green & Blue.



```
>> size(X1)

ans =

   533   400     3

>> size(X2)

ans =

   533   400     3

>> size(XFUS)

ans =

   533   400     3

fx >> |
```

Figure 3: Shows the Size of the Image1, Image2 and Fused Image



C:\Users\SIBICHAKKARAVARTI

D:\conference\IIT madras\Vomeg

Size: 119.90 KB

Height: 533 Pixel

Width: 400 Pixel

Can save: 563.01 KB

Encrypted image has been successfully saved.

Figure 4: Fused Image – Encrypted distorted portion is wrapped with the original image, 4x4 tiles denotes the fusion process, Where the standalone image denotes the steganography

V. CONCLUSION

Hence we conclude this paper with a new hybrid method for steganography with image fusion, which can be widely used in various applications for secured transmission. In the case of data transmission within the communication channel, information exchanged can be a media whether it may be an image or video files etc. Our Technique has an enormous count of advantages over other security techniques; our proposed methodology can be used to increase the security for the web based applications. The experimental results demonstrated here shows the pre-eminence of the proposed method.

VI. FUTURE ENHANCEMENT

Since our method leads has a load of memory weightage for Bitmap images of 32 bit. Hence in future the above mentioned challenge was considered and worked to achieve an optimal solution in steganography. The future enhancement of the proposed method is likely to be applied for video files so that it helps in video steganography along with video fusion

REFERENCES

[1]Sibi Chakkaravarthy S, Visu P, Kamalanaban E, VarunKumar K.A, ArunKarthick G, Kavitha k, StegFuse – Steganography and Image fusion for JPEG images", IEEE Int.Conference, ISCO 2014.

[2]Piyush Marwah, Paresh Marwaha(2010); "Visual Cryptographic Steganography in Images", Second International conference on Computing, Communication and Networking Technologies, 2010.

[3]Asad, M.; Gilani, J.; Khalid, A(2011); "An enhanced least significant bit modification technique for audio steganography"; ICCNIT 2011 IEEE.

[4]NaizhangFeng, Mingjian Sun, Liyong Ma, JiachenMa (2009); "Curvelet Based Image Fusion for Ultrasound Contrast Harmonic Imaging"; Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Page(s) 953-956.

[5]Dorairangaswamy M.A & Padhmavathi B(2009);"An Effective Blind watermark Scheme TENCON, IEEE.

[6]Amir Nooraliei and R. Iraji, Member (2010);"Noise reduction and image sharpening using IJA stochastic learning automaton"; Second International Conference on Computer Research and Development.

[7]ShuQinRen, JianCheng, Min Li (2010);"Multi resolution Fusion of Pan And Ms Images based On the Curvelet Transform", IGARSS.

[8]JianweiMa(2011); "Improved Iterative Curvelet thresholding for Compressed Sensing and Measurement", IEEE transactions on instrumentation and measurement, vol. 60, no. 1.

[9]Shadi AlZubi, MhdSaeed Sharif, Naveed Islam, and Maysam Abbod(2011); "Multi-Resolution Analysis Using Curvelet and Wavelet Transforms for Medical Imaging"; IEEE .

[10]Kiran Parmar and Rahul Kher(2012);"A Comparative Analysis of Multimodality Medical Image Fusion Methods"; Sixth Asia Modelling Symposium .

[11]CS(2004).http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf

[12] S.Sibi Chakkaravarthy, Reshmi R Nair and P.Visu(2013);" A Novel Methodology to identify and recognize the composite human gesture for Kinect based Human-machine interface" Science publication.

[13]Akhtar, N.; Johri, P.; Khan, S(2013) "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29.

[14]Yadav, P.; Mishra N, Sharma, S(2013) "A secure video steganography with encryption based on LSB technique," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1,5, 26-28.

[15]Kumar, R.P.; Hemanth, V.; Shareef, M.,(2013) "Securing Information Using Sterganoraphy," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on , vol., no., pp.1197,1200, 20-21.

[16] Verma, M.; Kaushik, V.D.; Rao, C.V.(2012) "Curvelet based image fusion," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.959,964.

AUTHOR

Arun Karthick G, currently pursuing M.Tech in the stream of Embedded System Technologies, at VelTech Dr.RR & Dr.SR Technical University and his past, Experienced with B.E. in Electronics and Communication Engineering .Currently working as the project intent at CDAC, Pune