5. Description of the Research Work

Data hiding provides easy way of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely. This system would be mainly concerned with the algorithm ensuring the secure data transfer between the source and destination. For that we first used encryption and then data hiding and vice-versa. In data hiding we will use cover image for security purpose. The medium in which information is to be hidden, is called as cover image.

The secret key use for encrypting the image and data hiding is same. To resolve that problem we will use one secret key for encrypting the image and another secret key for data hiding. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. Thus, if the both keys are different then there are lots of security in data transmission.

RGB shares are generated from the original secret image and by sticking together with encrypted image reveal the secret. If we are creating one or more shares and some or all of them sticked together for getting the real secret unreveal. This process of securing data is called as secret sharing. This is one of the secure process in secure data transmission. This improves the overall quality of an image.

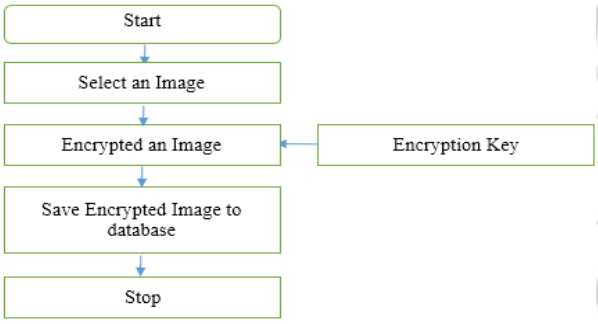

Figure 4.1: DFD for Training Phase

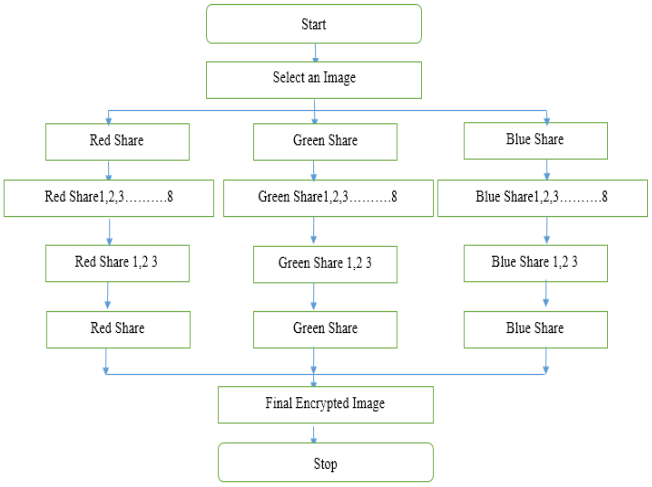

Figure 4.2: Proposed Image Encryption Method

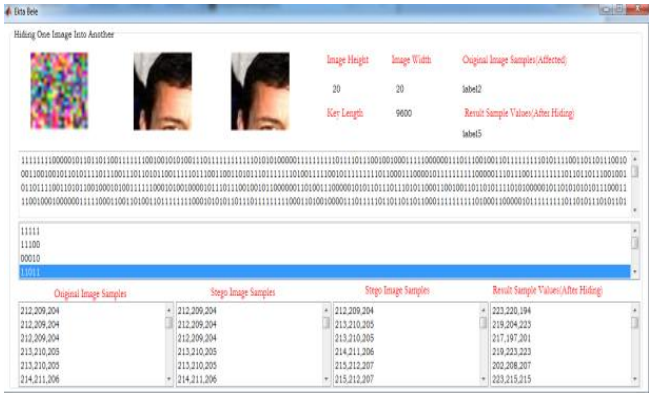

Figure 4.3: Data Hiding process

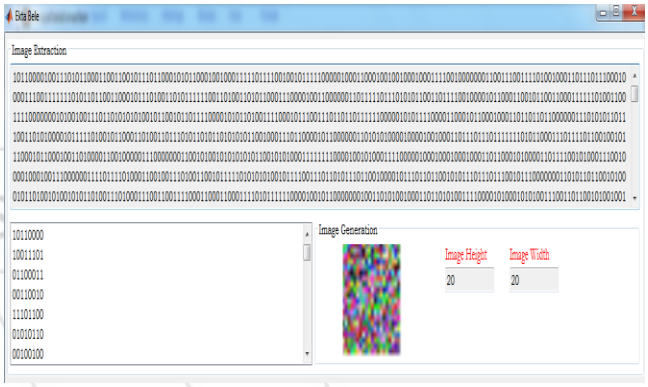

Figure 4.4: Data Extraction process

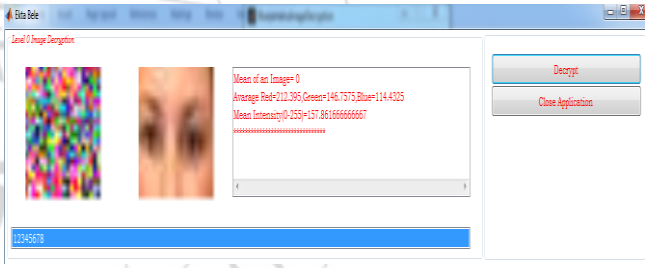

Figure 4.5: Data Decryption process

6. Conclusion

Although only some of the main steganographic techniques were discussed here, one can see that there exists a large selection of approaches to hiding information in digital media. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. So, our future study and research includes developing the data hiding methods with high embedding capacity & robustness. We present a reduced distortion formula for LSB image steganography. The key plan of the formula is knowledge activity bit embedding that causes minimal embedding distortion of the host image. visual image tests showed that delineate formula succeeds in increasing the depth of the embedding layer from 1th to 5LSB layer while not touching the sensory activity transparency of the info hided image signal. the advance in lustiness in presence of additive noise is clear, because the projected algorithmic rule obtains considerably lower bit error rates than the quality algorithmic rule. The steganalysis of the projected algorithmic rule is more

difficult similarly, as a result of there's a big cryptography provided for knowledge security.
hided image signal.

References

[1] V. Saravanan, A. Neeraja, "Security Issues in Computer Networks and Stegnography". 978-1-4673-4603-0/12/$31.00 ©2012 IEEE
[2] Xiang Wang, Qingqi Pei, Hui LiA "Lossless Tagged Visual Cryptography Scheme", IEEE Signal Processing Letter, Vol. 21, No. 7, July 2014.
[3] Souvik Roy and P. Venkateswaran " Online Payment System using Steganography and Visual Cryptography". 978-1-4799-2526. 1/14/$31.00 ©2014 IEEE
[4] Biswapati lana, Madhumita Mallick" Cheating Prevention in Visual Cryptography using Steganographic Scheme". 978-1-4799-2900-9/14/$31.00 ©2014 IEEE.
[5] Shubhra Dixit, Deepak Kumar Jain,Ankita Saxena "An Approach for Secret Sharing Using Randomised Visual Secret Sharing". 978-1-4799-3070-8/14 $31.00 © 2014 IEEE
[6] Akhil Kaushik, Krishan Gupta, Anant Kumar," Digital Image Chaotic Encryption ", International Conference on Reliability, Optimization and Information Technology – ICROIT 2014, India, Feb 6-8 2014
[7] wenjun lu, avinash varna, (member, ieee), and min wu," confidentiality-preserving image search: a comparative study between homomorphic encryption and distance-preserving randomization ", Digital Object Identifier 10.1109/ACCESS.2014.2307057, March 4, 2014.
[8] [8] Zafar Shahid and William Puech," Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings", ieee transactions on multimedia, vol. 16, no. 1, january 2014.
[9] [9] Nitumoni Hazarika, Monjul Saikia," A Novel Partial Image Encryption using Chaotic Logistic Map ", 2014 International Conference on Signal Processing and Integrated Networks (SPIN)
[10] [10] Geum-Dal Park, Dae-Soo Kim, Kee-Young Yoo," Lossless Codebook-Based Digital Watermarking Scheme with Authentication", 2014 11th International Conference on Information Technology: New Generations