International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Implementation of MLMS base Information Security in Combination with HLSB Data Hiding Method

Ekata S. Bele[1], Chetan Bawankar[2]

[1]WCEM Dongargaon, Nagpur, Maharashtra, India

[2]Professor, Head of CSE Department, WCEM Dongargaon, Nagpur, Maharashtra, India

Abstract: ***To assert the secrecy and confidentiality of pictures or image could be a vivacious space of analysis, with totally different approaches being followed, the primary being encrypting the pictures through multi share multi level algorithms mistreatment keys, the opposite approach involves activity information mistreatment higher lsb data activity algorithmic rule to keep up the pictures secrecy. A data content owner encrypts the important image by mistreatment totally different share, and a hide knowledge will add further knowledge into the encrypted image mistreatment higher lsb data-hiding technique although he doesn\'t understand the initial and real data. With an encrypted image containing further knowledge, a receiver could initial rewrite it consistent with the cryptography key, and so extract the embedded knowledge and recover the initial image consistent with the data-hiding key.***

Keyword: Cover image, data hiding, data extraction, Image encryption, Image decryption and Data recovery.

1. Introduction

Cryptography may be a technique for securing the key data. Sender encrypts the message exploitation the key sends it to the receiver. The receiver decrypts the message to induce the key data. Cryptography focuses on keeping the content of the message secret wherever as information activity concentrates on keeping the existence of the message secrete . information activity is that the different technique for secured communication. information activity involves activity data therefore it seems that no data is hidden in any respect. If an individual or persons views the article that the data is hidden inside he or she is going to haven\'t any concept that there is any hidden information, thus the person won\'t commit to rewrite the data.

Information activity is that the method of activity a secret message at intervals cowl medium like image, video, text, audio. Hidden image has several applications, particularly in today's fashionable, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly. The strength of data hiding gets amplified if it combines with cryptography.

The terminologies used in data hiding are cover-image, hidden image, secret message, secrete key and embedding algorithm. Cover-image is the carrier of the message such as image, video or audio file. Cover-image carrying the embedded secret data is the hidden image. Secret message is the information that is to be hidden in a cover image. The secret key is used to embed the message depending on the hiding algorithm . The embedding algorithm is the way, which is used to embed the secret information in the cover image.

2. Literature Survey

Shyong Jian Shyu [2014] introduced 2 novel and effective VCRG-GAS algorithms to resolve the matter of visual secret sharing for binary and color pictures. during this paper the algorithms don't need any additional component growth. Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin carver [2014] planned easy visual secret sharing theme, not solely maintains the protection and component non-expanding advantages of the random-grid technique, however conjointly permits for the assembly of purposeful share-images, whereas satisfying the wants of being simple to hold and simple to manage. Moreover, all pixels within the cover-image and therefore the secret image square measure wont to perform cryptography, that ensures that the distinction on the share-images and therefore the stack-image will reach the theoretical most. This technique conjointly removes some uncalled-for cryptography restrictions (e.g., having to use only 1 cover-image, having to require enough black pixels from the key image) that makes the cryptography method a lot of versatile. The findings show that our easy visual secret sharing is healthier than the strategy. This technique makes the info embedding method to change a lot of LSBs of a constituent supported region sort to extend the capability of the stegnography. additionally the planned technique makes the steganalysis onerous. thence the protection, capability and doctor's degree can get improve. In future the face detection algorithms are often superimposed to our planned technique to extend the capability of the stegnography method while not increasing doctor's degree. Visual. Javelin Strategy & analysis, [2013]Identify Fraud Report, steganography and visual cryptography that has client knowledge privacy and prevents misuse of knowledge at merchant's facet. the tactic worries only with bar of establish stealing and client knowledge security. as compared to different banking application that uses steganography and visual cryptography square measure primarily applied for physical banking, the planned technique will be applied for E-Commerce with focus space

on payment throughout on-line searching similarly as physical banking.

Stacking the pretend Share with all different share includes S l , it'll show the pretend image, and once stack the pretend Share with all different shares excluding SI then show overlapping image of original image and pretend image This is as mentioned earlier is known as Partial Cheating, creates the confusion between the users regarding original image. this sort of cheating is completed by a Malicious Participant. it's terribly simple for a Malicious Participant to cheat others as he is aware of the dimensions of the share and might simply develop a faux share with the assistance of a faux image and his share. faux share are often detected by checking the message, embeded at intervals it with non everification share. The system are often improved by embedding secret message in column major to completely different share, so we will provide the priority to every share. Priority primarily based VC are often utilize in completely different organization which may be developed in future.

We focus on detecting data hiding in motion vectors of compressed video and propose a new steganalytic algorithm based on the mutual constraints of motion vectors. The constraints of motion vectors from multiple frames are analyzed and formulized by three functions, then statistical features are extracted based on these functions. Moreover, we also incorporate calibration method to improve the detection accuracy. Experimental results demonstrate that the proposed method can effectively attack typical motion-vector based video steganography

The network provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. Steganography and cryptography are two different data hiding techniques. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message. We propose a high capacity data embedding approach by the combination of Steganography and cryptography. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. A comparative analysis is made to demonstrate the effectiveness of the proposed method by computing

Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). We analyzed the data hiding technique using the image performance parameters like Entropy, Mean and Standard Deviation. The stego images are tested by transmitting them and the embedded data are successfully extracted by the receiver. The main objective in this paper is to provide resistance against

3. Problem Definition

A new challenge consists to enter information in encrypted pictures. Since the entropy of encrypted image is peak, the embedding step, thought-about like noise, isn't potential by victimisation customary information concealing algorithms. a replacement plan is to use reversible information concealing algorithms on encrypted pictures by desire to get rid of the embedded information before the image cryptography. There was another downside if either {of information of knowledge of information} concealing key or coding key's leaked then the unwelcome person will extract or decipher the image through data concealing key or decipher the image through coding key.

Another drawback found is that, the key key use for encrypting the image and knowledge concealment is same. therefore the user World Health Organization is aware of the key key use for encoding will access the embedded knowledge and original knowledge. the initial image is retrieved from encrypted image when extraction or removing the information hidden within the image. The content owner and knowledge hider share identical encoding key for encoding of image and knowledge concealment.

In previous work , there aren't any provision of selecting the key and a lot of encode-decode time consumption. There ar countless knowledge concealment programs offered. many of them ar wonderful in each respect; sadly, most of them lack usable interfaces, or contain too several bugs, or inconvenience of a program for alternative in operation systems.

4. Proposed Method

To enhance the embedding capacity of image steganography and provide an imperceptible stegoimage for human vision, we propose a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access. Steganography also can be implemented to cryptographic data so that it increases the security of this data [4]. In this method we first encrypt a message using transposition cipher method and then embed the encrypted message inside an image using LSB embedding method. Hiding data using LSB modification alone is not highly secure. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding method to decipher the encrypted message. One of the most important features of lossless compression is to maximize the embedding capacity.

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.

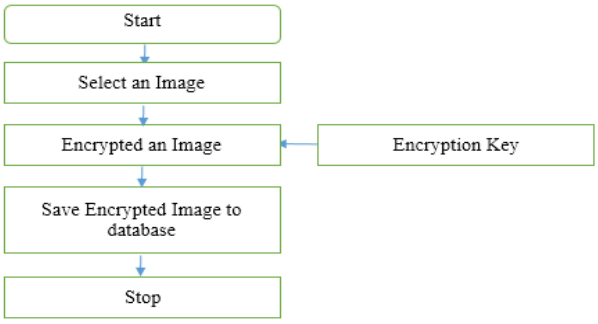

Figure 4.1: DFD for Training Phase

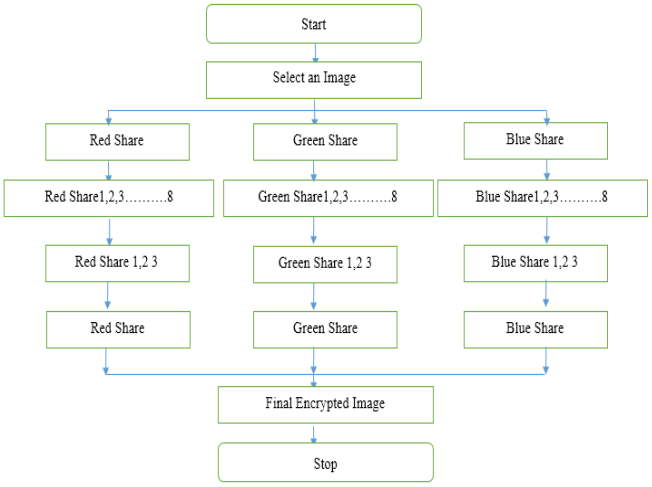

Figure 4.2: Proposed Image Encryption Method

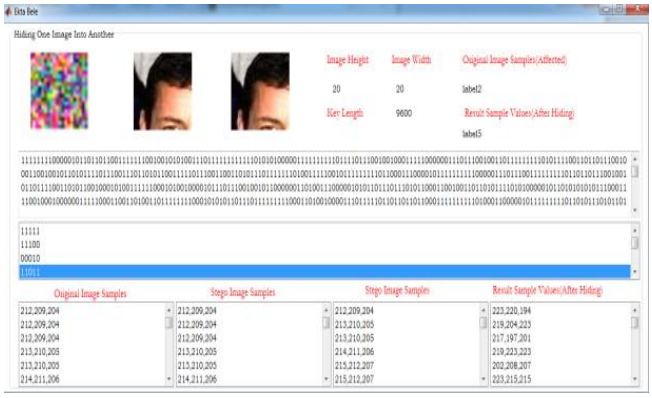

Figure 4.3: Data Hiding process

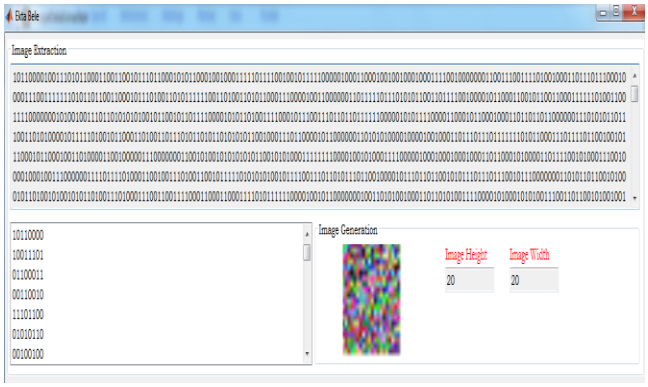

Figure 4.4: Data Extraction process

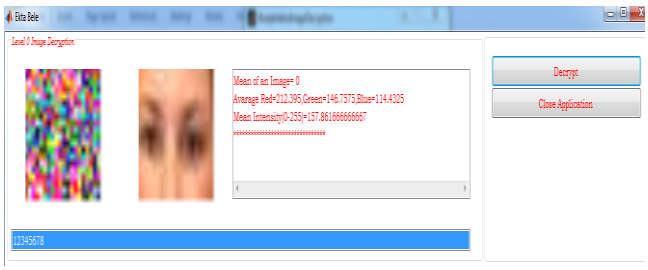

Figure 4.5: Data Decryption process

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