November-December 2019
ISSN: 0193-4120 Page No. 6348 - 6350

Smart Image Security using Image Processing Techniques

V. S. S. P. Raju Gottumukkala, N. Kumaran, V. ChandraSekhar
V.S.S.P.Raju Gottumukkala,Research Scholar,CSE Department,Annamalai University,Annamalai Nagar , Tamilnadu, India.(email: vssprajug@gmail.com)
Dr. N. Kumaran, Assistant Professor,CSE Department,Annamalai University, Annamalai Nagar, Tamilnadu, India.
Dr. V. ChandraSekhar,Associate Professor,CSE Department,S.R.K.R.Engineering College,Bhimavaram, A.P. India.

Article Info
Volume 81
Page Number: 6348 - 6350
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *28 December 2019*

Abstract:

Image Security is an area of research which needs much attention these days in the era of electronic information exchange. Information Security has been a wide area with range of techniques. But still image encryption is yet another area of concern. With wide usage of cheaper mobile cameras and wide exchange of personal images, ensuring privacy is indispensable. There are many techniques that involve encryption, watermarking, Visual Cryptography, steganography etc., Still manipulating images at the level of local parameters like pixel, texture, geometry, clarity, locality etc., will ensure better security of image information. Banking, Consultancies, Detective agencies, Defense forces are all looking for such techniques to secure their information transfer. In proposed system, the images are encrypted, the needful information is embedded and hidden at the senders end. The receiver has to reverse the process to recover the information.

Keywords: *Image Processing, Machine Learning, Information Security, Image Security etc.*

I. INTRODUCTION

Electronic Information Exchange is order of the day. Many mobile applications and web applications look for better ways to secure the images because of popularity of the apps which are used to exchange images like Instagram, etc., There are many techniques that involve encryption, watermarking, Visual Cryptography, steganography etc., Still manipulating images at the level of local parameters like pixel, texture, geometry, clarity, locality etc., will ensure better security of image information. Banking, Consultancies, Detective agencies, Defense forces are all looking for such techniques to secure their information transfer.

Image processing is an area of study that allows analysis and manipulation of images in digital format to improve its quality or manipulates it for some purpose of study. Image processing can help in image security with techniques like image stitching, steganography etc., Using such techniques information can be encoded into images and such encrypted images usually not visible to human eyes which is a huge advantage. It can't be decrypted without tools designed for the specialized purpose. Usually the secret image is segmented to many parts and encrypted secret message is embedded into images, then the hiding of this information happens to camouflage the text. At receivers end the images are received, and the hidden information is decoded then decrypted. The application of image stitching of the segments can help further to avoid man in the middle attacks.

Machine learning is a technique that is inseparable from image processing in the field of computer vision. Machinelearning is used in image processing or computer vision because optimizes differentiable parameters so that cost or loss functions can be minimized. It comes in handy with pattern recognition problems especially. Machine learning algorithms especially the nearest neighbor techniques can help in resolving the image stitching problems. Stitching is putting several parts of images to incorporate a bigger image. It can be different images too.

Information security techniques are very much mandatory in this field because they are used for encryption and decryption of information that goes with the images. It ensures in protecting against unauthorized use of the digitized information. All these techniques can ensure better security of the information that is transferred.

November-December 2019
ISSN: 0193-4120 Page No. 6348 - 6350

II.RELATED WORK

The related work by contemporary authors is discussed in this section. There have been various techniques especially on following genres to implement image security.

a) Visual Cryptography
b) Water Marking
c) Steganography
d) Encryption

The summary of past works in these areas is summarized here.

Yu et al(2018) [1] suggest their study in Visual analytics. The survey for deep learning to help users better understand this field. The author presents a survey addressing the requirement of all types of stake holders and the describing the concepts of deep learning, organizing a assessment structure for the architecture, debugging and supporting structures, concepts to increase the efficiency and effectiveness of the model.

Fernandez et al(2018) propose[2] their work on ColorCheckers which are reference standards. This gives suggestions to the users to improve the images as input considering the lighting of the background. The work goes for automatic detection of such information and helps in improving the image input. The localization and patch recognition are two parts of the work.

Hofbauer et al(2016) propose their[3] work in Visual security metrics. It is mandatory to also know if the security is good enough. The metrics help in this direction.

Evaluation of the visual security is done with respect to quality of the images etc Several metrics and techniques are involved in the system.

Temel et al(2019) analyze the statistics [4]of error signals. It is used in order to improve the quality of the images. It considers the scaling of images in order to find error signals in the images. Three databases and thirty types of distortions are used in order to perform the task. Several standard algorithms are considered for comparison. There are five metrics considered like linearity, monotonicity, accuracy, and consistency.

Loh et al(2019) They[5] show the effect of low lighting and their effects in the input images. The concept of illumination invariance is discussed herein. The noise based problems associated to lighting are discussed in this work. Neural networks and artificial intelligence concepts are used in to materialize the concept. Thus improving the image quality in low light is discussed.

Tayeb et al(2015) [6]describe a modified segmentation method applied to image. The expectation and maximization concepts of machine learning are deployed here. The goal is to improve the computational cost. Segmentation is the allied area where the concept is deployed. The error during classification and pattern recognition is resolved here. Each object is found and compared in this regard. Segmented sections and comparisons are highly challenging when pattern matching.

Zaitoun et al(2015)[7] present a comparative analysis. Block based segmentation is considered here. The pdf input is considered here. Region and boundary are main concerns in this work. The results are evaluated both by subject experts and automated systems in order to evaluate the results. The results prove to better to avoid discrepancy.

Mageshwari et al(2013) present[8] a study on different image segmentation techniques based on parameters like threshold, region based segmentation, edge based segmentation etc., The proposed work is implemented using MATLAB and the Sobel and canny edge detection algorithms are applied here. The accuracy of classification is improved by filtering the features in terms of entropy.

Harbach et al(2016) present a [9]detailed analysis of the smartphone locking mechanisms. These are discussed to be generically applied to all types of smart phones. Pattern matching for device unlocking is the perspective here. The image security based technique is evaluated in terms of number of unlock error user performs, duration involved etc.,

Hu et al(2018) have taken up [10]the security of image with steganography. This performs steganalysis considering the traditional techniques of image embedding and hiding. And machine learning framework for detection of the embedded images are considered for evaluation. But without embedding the system performance is shown to increase in terms of security in this system.

Delon et al(2005) suggest in this paper, [11]a new method for the segmentation of color images is presented. This method searches for segments based on histograms and their intensity. An automatic color recognition system to accurately match colors is an addition to the existing system.

The new technique involves image color histogram to perform analysis.

Hoover et al(1996) propose[12] a methodology for evaluating range image segmentation. Identifying the geometry based image noise region, correctly segmented, missed regions are also evaluated. A reference dataset is used but the prototype can be applied for real time dataset.

Andriotis et al(2013) suggest [13]about the Graphical passwords that allow a user to unlock a smartphone's screen are one of the Android operating system's features and many users prefer them instead of traditional text based codes. Since there are variety of attacks to recover the patterns or passwords. The author presents a survey on the types of attack like behavior based ones and how to reduce the search area to identify proper patterns for improving the lock mechanisms.

Li et al(2018) have addressed the [14]need for information security in their work. Iris based biometric recognition is area of concern here. Based on this image encryption is considered here. Deep learning is used for image classification and feature selection. Image encryption and decryption are performed to improve the results thereby.

Thus the contemporary works are presented in this section.

III.PROPOSED WORK & RESULTS

In proposed system, the source image is segmented into various parts. There are usually Encryption phase, Embedding phase and Hiding phase. The segmented parts of the image are looked upon as image stitching parts. The text information is encrypted, then embedded in images in

hidden format. Finally in decryption phase the reverse process happens and the image stitching is reversed to rebuild the image to see the whole information. Here if anyone interferes the digital communication, segments of images are not comprehensible and the whole information is understood only by putting things together. There is scope for improving the security by improving the encryption process or the machine learning process to locate the segments and resolve the problem. Thus the research is headed towards improving the image security using image processing.

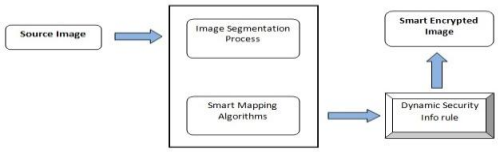

Fig 1: System block Diagram

The following[15] is the algorithm for image stitching which helps in the final outcome.

i. Consider an image instance and mark its features.

ii. Euclidean distance between two image instances in calculated

iii. The formula is

d(xi,xj)=sqrt(sum for r=1 to n(ar(xi) – ar(xj))2)

iv. For each image the following is performed

v. Extract the features of interest from all n images

vi. Perform focal length adjustment to correct the lighting and related issues.

vii. Perform filtering to avoid noise component.

viii. For each feature of each instance perform k-nearest neighbor algorithm

ix. For each image match the features using RANSAC algorithm

Thus the proposed system is explained in detail. The following is a comparison of the performance of some algorithms in existing methodologies. The proposed work tries to make betterment compared to these algorithms.

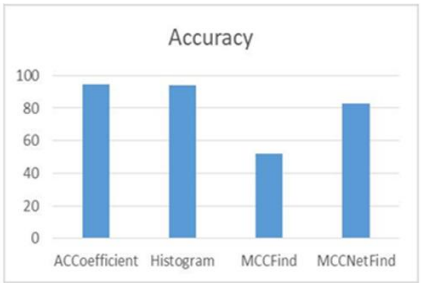

Fig 1: Comparision of Algorithms

IV.CONCLUSION

The proposed work on Image Security using Image Processing is a promising technique in terms of better Security. The proposed work presents a detailed survey of existing techniques, compares their performance. Image Security using Image Processing using prominent techniques like image stitching etc., is highly relevant in electronicinformation exchange. The proposed work can be extended in terms of deep learning techniques for better performance..

REFERENCES

1. Rulei Yu, Lei Shi, “A user-based taxonomy for deep learning visualization”, Elsevier, Science Direct ,Visual Informatics, Vol 2 ,2018,pp- 147–154
2. Pedro D. Marrero Fernández, Fidel A. Guerrero Peña , Tsang IngRen, Jorge J.G. Leandro,” Fast and robust multiple ColorChecker detection using deep convolutional neural networks”, Elsevier, Science Direct ,Image and Vision Computing , Vol 81, 2019,pp- 15–24
3. Heinz Hofbauer , Andreas Uhl,”Identifying deficits of visual security metrics for images”, Elsevier, Science Direct ,Signal Processing: Image Communication, Vol 46, 2016,pp- 60–75
4. DogancanTemel , GhassanAlRegib,” Perceptual image quality assessment through spectral analysis of error representations”, Elsevier, Science Direct ,Signal Processing: Image Communication, Vol 70, 2019,pp- 37–46
5. Yuen PengLoh, CheeSeng Chan,” Getting to know low-light images with the Exclusively Dark dataset”, Elsevier, Science Direct ,Computer Vision and Image Understanding , Vol 178 ,2019,pp- 30– 42
6. LahouaouiLalaouia, Tayeb. Mohamadib , and AbdelhakDjaalabb,” New Method for Image Segmentation”, Elsevier, Science Direct ,Procedia - Social and Behavioral Sciences , Vol 195, 2015 ,pp- 1971 – 1980
7. Nida M. Zaitoun, Musbah J. Aqel,” Survey on Image Segmentation Techniques”, Elsevier, Science Direct ,Procedia Computer Science, Vol 65, 2015,pp- 797 – 806
8. UmaaMageshwari, Sridevi.S, Mala.C,”An experimental study and analysis of different image segmentation techniques”, Elsevier, Science Direct, Procedia Engineering , Vol 64 , 2013,pp- 36 – 45
9. Marian Harbach, Alexander De Luca, Serge Egelman,” The Anatomy of Smartphone Unlocking- A Field Study of Android Lock Screens”, ACM, Privacy and Security Interfaces, 2016,pp-4806-4817
10. Donghui Hu , Liang Wang, Wenjie Jiang, ShuliZheng , And Bin Li,” A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks”, IEEE Access, Vol 6, 2018, pp-38303-38314
11. Julie Delon, Agnes Desolneux, Jose Luis Lisani, and Ana Belen Petro,” Color Image Segmentation Using Acceptable Histogram Segmentation”, J.S. Marques et al. (Eds.): IbPRIA 2005, LNCS 3523, pp. 239–246, 2005
12. Adam Hoover, Gillian Jean Baptiste, Xiaoyi Jiang, Patrick Flynn,HorstBunke, Dmitry Goldgof, Kevin Bowyer, David Eggert, Andrew Fitzgibbon, Robert Fisher, “An experimental Comparison of range image segmentation algorithm”IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 18, No 7, 1996, pp 673-689
13. PanagiotisAndriotis, Theo Tryfonas, George Oikonomou, Can Yildiz,” A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks”,ACM, WiSec’13, April 17-19, 2013, Budapest, Hungary,pp-1-6
14. Xiulai Li, Yirui Jiang, Mingrui Chen and Fang Li, “Research on iris image encryption based on deep learning”,EURASIP Journal on Image and Video Processing, 2018, vol-126, pp – 1-10
JyothikaKapur, AkshayJ.Baregar, “Security using Image processing”, International Journal of Managing Information Technology, Vol 5, No 2, May 2013, pp-13-21