A SECURE AND HIGH CAPACITY IMAGE STEGANOGRAPHY TECHNIQUE USING IWT AND DCT

MOHD.ABDUL.KHADER .KHAN[1],
Dr.SYED ABDUL SATTAR[2]

[1]Research Scholar, CMJ University, Meghalaya, India

[2]Professor & Dean of Academics, Royal Institute of Technology & Science, Andhrapradesh, India

E-Mail: khader_all@yahoo.co.in

Abstract

The current technique suggest a new methodology for making a "secure steganographic strategy" utilizing visual cryptography& GA (genetic algorithm)aimed at robust encryption in computer forensics. Despite there is a general research work in previous days, however greater part of research work does not have much optimal consideration aimed at robust safety towards encrypted picture. The recommended system encodes the secret message in slightest important bits of real picture, whereas the encrypted picture pixel values would change with the use of GA to recollect their statistic characters, therefore creating the identify secret message is problematic. GA utilization has required the framework to upgrading the security utilizing mutation, optimal selection, &cross over. The suggested framework hides information in an original picture and attains its identification then afterward under went to visual cryptographic. The execution will be done in matlab that reveals that the recommended framework has superior resilience by recognizing bench marking and Steganalysis with optimal visual principles.

Keywords-Steganography, Visual Cryptography, Genetic Algorithm, RS Analysis

I. Introduction

A system that empowers to have a secret correspondence in current methodology utilizing steganography, which is also known as public channel. The RS study will be recognized as a most popular steganalysis procedure that has possibility to identify the unseen message by fact examination about pixel values [1]. The methodology of RS steganalysis utilizes the singular & general groups as considerations to calculate the pixels correlation [2]. The correlation of robust existence has been witness in contiguous pixels. However, unfortunately utilizing conventional LSB replant steganography [3], the framework renders modification in regular & singular gatherings that exposes steganography existence. Ultimately, it will not be much tough to decrypt secret message. Both visual cryptography & steganography topic has been recognized as dissimilar subject for picture safety. Despite there are wide researches relay on joining these 2 methodologies [4] [5] [6], however, the outcomes are not much acceptable w.r.t RS study. Other traditional techniques of picture security has seen the utilization of advanced watermarking extensively that embeds an alternate picture inside an picture and then utilizing it as secret picture [7].The utilization for steganography for mix visual cryptography will be a robust method and includes some challenges to detect encrypted & unseen data. Basically, one can have a secret picture with private information that might be dividing into different encrypted shares. Lastly, when encrypted shares are decrypted or reunited to update the real picture it is probable for one to have an uncovered picture that yet comprises of private information. Such sorts for algorithms can't persevere without possessing suitable qualities in visual cryptography process. The ground for this is that whether the modifying system or significantly encoding strategy progressions the information exists in picture, after that the framework might consequently change the encrypted data which makes framework attainable to extracting the encrypted information from the presented picture.

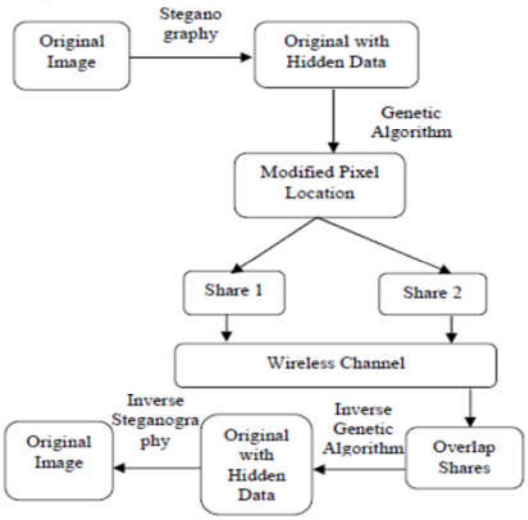
The steganalysis is the transform with uncover the private message Indeed going specific questionable networking. There need aid Different strike accounted for slightest critical Bytes substitution about picture components alternately touch planes [8][9]. Different histogram and also piece impact need also been accounted for in the former examination fill in [10]. Anyway specific RS steganalysis fill in need been accounted Similarly as the vast majority cement and proper system on other accepted substitution steganography [11], which employments standard Furthermore solitary bunches Likewise those Primary parameters will assess the companionship of the pixels. In place will keep RS analysis, the effect on the affiliation of the pixels will a chance to be obliged with be adjusted. Such sorts of payment could a chance to be finished toward changing different touch planes. Toward completing such attempt, those suggestions towards security will a chance to be Just about computationally incomprehensible. To such reason, different streamlining calculations might make deployed utilized over secure information concealing will recognize the ideal embedding positions. The principle point of recommended model should outline a practical RS- imperviousness secure procedure that combines the utilization about both steganography Furthermore visual cryptography with objectives about enhancing security, reliability, Also effectiveness for mystery message.

II. Literature Review

Ghascmict al. [12] recommended a new steganography plan dependent upon GA & integer wavelet transform. Umamaheswari proposed the secret message & encrypt it with the use of public key of receiver along with stego key & embed both messages utilizing an embedding method. Shyamalendu Kandar recommended a system from claiming great referred to k-n secret imparting for color pictures utilizing a variable length key with stake division utilizing irregular amount. Anupam depicts how such an even-odd encryption based on value of ASCII will be connected and how encrypted message converting toward utilizing Gray code and embedding with picture could secured the message and therefore creates job of cryptanalyst problematic.

III. Proposed Method

The recommended work will be fundamentally a schema intended in java swing with 2 components, for instance, Visual cryptography and GA. An input picture will be acknowledged as cover picture to input message in format of plain text. Following embedding the “secret message in LSB (least significant bit)” of cover picture, the steg picture pixel values are changed towards visual cryptography to keep their statistic characters. The evaluation outcomes must demonstrate the recommended algorithm’s viability in safety to steganalysis with finer visual eminence. The client might choose their focused majority of the data in terms of plain content for embedding secret message in LSB of cover picture. The suggestions of visual cryptography are empower the steg picture pixel values to stay their statistic character. LSB steganography has “high embedding capacity & low computation complexity”, in which a “secret binary sequence” will be utilized to displace the “low significant bits of host medium”. This will be the robust method that stores the data evidence from any interloper.



IV. Methodology

The recommended work contain 2 algorithms, they are (i) Visual cryptography with pseudorandom number (ii) Steganography utilizing GA. The provision initiates with Steganography component where the cover picture is encrypted to produce the Stego picture. The stagographic picture produced in this component is act like input for to “visual cryptographic module”.

The suggested method will be built on “standard visual secret sharing & visual cryptography”. The applied strategy utilizes the pixels exchange & pseudorandom number allotment. The different segment of this execution is that while decrypting the stego picture is morphologically same contrasted with cover picture w.r.t the size & shape thereby preventing the expansion effect of pixel. The execution of the algorithm produces the good outcome with inconsequential shares when stego pictures would regularly with contrast of light. It might also be seen that the algorithm provides much darker shares in colored & gray output.

V. Results & Analysis

The proposed work will be designed on “32 bit Windows OS with Dual Core Processor with 2 GB RAM and 1.80GHz using Matlab Platform”. The real picture will be in “JPEG format of 5.28KB where the plain text message size 569 bytes” is represented in Figure 1.

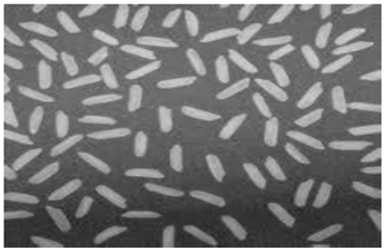


Figure.1. Original Image

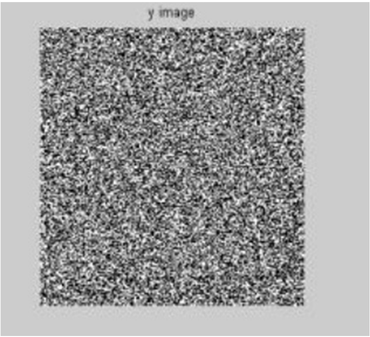


Figure.2. Shares of Stego Image

The encrypted procedure will be carried out utilizing the GA deploying use of “BattleSteg, Blind Hide, Filter First, and Hide Seek algorithm”. The encryption might also support to provide the PNG format of stego picture of 85.4KB is represented in figure 2. And prevent the analysis of RS, it might also display the picture in “complete black pixels for blind steganalysis”, whereas the embedded picture will be also in same PNG format.

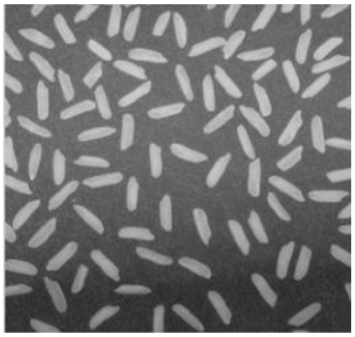


Figure.3. Stego Image Analysis

The recommended system encrypts secret message that will be very insignificant for every square of picture. The procedure only encrypts 1 byte in 8x8 blocks same time other traditional methods utilizes 1 bit in every pixels. Consequently, this procedure might be utilized for “encrypting secret message for every block of picture” that fundamentally enhances the execution and recollects a better quality of picture during encryption. The vital element in regards to the suggested framework is that it doesn't rely on upon the encryption of data in LSB of pixel qualities. The method continuously endeavor to assess the optimal private picture components whereas the layer of the cover picture component values will be corresponding in the raised layers of the picture thereby recollecting the prevalence of the picture that makes it totally safe against attack of RS.

The stego picture produces from the steganographic component is then subjected to our visual cryptography component that produces 5 secret shares as represented in Figure 3. The recommended “visual cryptographic component” is prolonged to work colored & gray scale picture in the “overlay picture utilizing threshold picture hiding system”.

The “colored stacked shares” are displayed in Figure 5. The importance of the recommended method will be that a customer might select the secret image location to allot to a private intensity and thereby the scheme incurs a supple and cooperative to selection of customer. Though, this procedure cannot be imagined an optimal secure associated to other approaches as specific levels of the confidentiality might yet be uncovered even whether the customer does not have possession of all secret shares, never the less it is almost impossible for anyone who will try to decrypt the encrypted data within that picture to expose whether the secret shares that they possess are set of all encrypted shares or specific secret shares are missing.

The presentation of the recommended framework will be investigated by executing the steganalysis and detecting the probabilities of RS analysis. The presentation is distinct by 3 factors, they are (i) Understanding "RS analysis factors for overlapping and non- overlapping groups of pixels", (ii) The "Laplace Graph with frequency variation consistent to Laplace value", and (iii) conducting benchmarking test for analyzing factors such as "Average Absolute Difference, Mean Squared Error, Laplace Normalization, Laplacian Mean Squared Error, Signal to Noise Ratio, Peak Signal to Noise Ratio, Normalized Cross- Correlation, and Correlation Quality" are represented in below tables.

S. No	Percentage Description	Percentage Value	Approximate Length
1	Red	1.9	375.6
2	Green	4.7	902.4
3	Blue	8.62	1761.1

Table.1. Non overlapping RS analysis

S. No	Percentage Description	Percentage Value	Approximate Length
1	Red	2.8	542.8
2	Green	6.5	1231.6
3	Blue	10.4	1973.8

Table.2. Overlapping RS Analysis

S. No	Frequency	Value
1	0.12	0.0
2	0.01	1.0
3	0.03	2.0
4	0.14	3.0
5	0.03	4.0
6	0.02	5.0
7	0.09	6.0
8	0.02	7.0
9	0.02	8.0
10	0.03	9.0
11	0.01	10

Table.3. Laplace Graph

S. No	Description	Value
1	Average Absolute Difference	0.003
2	Mean Squared Error	0.007
3	LpNorm	0.002
4	Laplacian Mean Squared Error	3.76
5	Signal to Noise Ratio	4.75
6	Peak Signal to Noise Ratio	1.23
7	Normalized Cross-Correlation	0.99
8	Correlation Quality	193.1

Table.4. Benchmark Tests

The above tables represent the association with picture safety along with quality of picture. As the visual quality of the subsequent pictures in steganography is of superior quality, there is no need of utilizing any outside adjustment.

Conclusion

The current system has examined execution of safely utilizing steganographic strategy utilizing visual cryptography and GA utilizing pseudorandom number. It could be closed that when typical picture security utilizing visual cryptographic method and steganographic will be applied, it makes the investigators unfeasible task to decrypt encoded secret message. The security characteristics of the steganographic are extremely optimized utilizing GA. The suggested framework will be extremely tough against attack of RS and optimally utilized for both colored output & gray scale in visual secret messages building it extremely companionable for real time applications. The upcoming work might be towards the upgrading the method utilizing neural system for the visual cryptography, thus that the framework might produce exceedingly imperceptible secret messages utilizing specific set of training data that can be robotically produced and is arranged following the task has been executed. Such kind of methodology can render the greater part secure visual cryptographic plan and steganographic.

Reference

[1] Fridrich, J., Goljan, M. and Du,R, Reliable Detection of LSB Steganography in Color and Grayscale Images, Proceedings of ACM Workshop on Multimedia and Security, Ottawa, October 5, 2001, pp.27-30.

[2] Sathiamoorthy Manoharan, an empirical analysis of rssteganalysis, proceedings of the third international conference on internet monitoring and protection, ieee computer society washington,2008

[3] Singh, K.M.; Nandi, S.; Birendra Singh, S.;ShyamSundar Singh, L.;Stealth steganography in visual cryptography for half tone images, Computer and Communication Engineering, International Conference, 2008

[4] JitheshK,Dr.AVSenthilKumar,MultiLayerInformationHiding,BlendOfSteganographyAndVisualCryptography,JournalofTheoritical and Applied Information Technology,2010

[5] HsienhuWu;ChweihyongTsai;ShuhuanHuang;,Coloreddigitalwatermarkingtechnologybasedonvisualcryptography,NonlinearSignal and Image Processing, IEEE-Eurasip,2005

[6] R.Chandramouli,NasirMenon,AnalysisofLSBBasedImageSteganographytechniques,IEEE-2001

[7] ArezooYadollahpour, HosseinMiarNaimi, Attack on LSB Steganography in Color and Grayscale Images Using Autocorrelation Coefficients, European Journal of Scientific Research ISSN 1450-216X Vol.31 No.2(2009),

[8] Qing zhong Liu, Andrew H. Sung, Jianyun X, Bernardete M. Ribeiro,." Image Complexity and Feature Extraction for Steganalysis of LSB Matching", The18thInternationalConferenceonPatternRecognition (ICPR'06)0-7695-2521-0/06$20.00©2006IEEE.

[9] J. Fridrich, M. Goljan, and D. Hogea. Steganalysis of jpeg images: Breaking the f5 algorithm. In Proc. of the ACM Workshop on Multimedia and Security 2002.

[10] AderemiOluyinki,SomeimprovedgeneticalgorithmsbasedonHeuristicsforGlobalOptimizationwithinnovativeApplications,Doctorialthesis, 2010

[11] TalalMousaAlkharobi,AleemKhalidAlvi,NewAlgorithmForHalftoneImageVisualCryptography,IEEE2004

[12] Chin-Chen Chang; Iuon-Chang Lin; , A new (t, n) threshold image hiding scheme for sharing a secret color image, Communication Technology Proceedings, ICCT2003.