JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A NOVEL PICTURE STEGNOGRAPHIC APPROACH FOR HIDING TEXT IN COLOR IMAGES THROUGH HSI COLOR MODEL

RINI ELIZABETH CHERIAN,
Research Scholar,
Department of CS & IT,
Sabarmati University,
(Formerly, Calorx Teachers' University),
Ahmedabad, Gujarat-382481, India.

DR. ASHISH CHATURVEDI,
Registrar,
Sabarmati University,
(Formerly, Calorx Teachers' University),
Ahmedabad, Gujarat-382481, India.

Dr. Mukta Agarawal,
Associate Professor,
Sabarmati University,
(Formerly, Calorx Teachers' University),
Ahmedabad, Gujarat-382481, India.

Abstract : Picture "Steganography" is the most common way of installing message in pictures with the end goal that its reality can't be identified by "Human Visual System (HVS)" and is known distinctly to sender and collector. The paper presents a novel methodology for picture "Steganography" utilizing "Hue-Saturation-Intensity (HSI)" shading space dependent on "Least Significant Bit (LSB)". The proposed strategy changes the picture from "RGB" shading space to "Hue-Saturation-Intensity (HSI)" shading space and afterward implants privileged information inside the "Intensity Plane (I-Plane)" and changes it back to "RGB" shading model subsequent to inserting. The said strategy is assessed by both abstract and Objective Analysis. Tentatively it is tracked down that the proposed strategy have bigger "Peak Signal-to Noise Ratio (PSNR)" values, great impalpability and numerous security levels which shows its prevalence as thought about over a few existing techniques.

KEY WORDS: "Cryptography", "Image Steganography", "Security in digital systems", "HSI shading model", "LSB",

I. INTRODUCTION

The word "Steganography" is gotten from two Greek words; "stegano" which means ensured and "graphia" which means composing. It very well may be characterized as the most common way of composing messages in a manner by which the presence of mystery message is known distinctly to sender and collector. "Steganography" require a transporter object, restricted information and installing calculation. It might likewise require an encryption calculation and mystery key at times to build the security levels of "Steganography". Utilizations of "Steganography" incorporates secure transmission of highly confidential reports among public and worldwide governments, getting internet banking and casting a ballot frameworks, secret correspondence among crooks and fear based oppressors and sending Trojan ponies and infections to assault on frameworks and so forth.

II. "STEGANOGRAPHY" VS "CRYPTOGRAPHY"

"Steganography" and "Cryptography" the two strategies are utilized for information secrecy (security of data from undesirable parties). However there likewise exists a few contrasts between them that is depicted underneath.

1. "Cryptography" is the training and investigation of secure correspondence yet "Steganography" is a craftsmanship just as a study of incognito correspondence.
2. The primary focal point of "Cryptography" is to keep quiet while "Steganography" means to stay discreet.
3. Security in "Cryptography" is accomplished by changing over the privileged information into non-reasonable structure while in "Steganography"; security is accomplished by concealing information in clearly innocuous transporters to shroud the presence of information.
4. "Cryptography" gives us secure correspondence by utilizing a key to peruse the data. A gatecrasher can't eliminate the pre-owned encryption however he/she can undoubtedly adjust the scrambled record and can make the encoded document inane which can't be handily perceived by the beneficiary. Then again, "Steganography" give us a technique for secret correspondence that can be eliminated just if the transporter object, in which information has been inserted, is changed. The privacy of covered up information will stay for what it's worth, until and except if a dubious client is prevailed with regards to discovering a strategy for distinguishing it.
5. The last undertaking of "Cryptography" is a code text yet the last yield of "Steganography" is a stego object.

6. To break the "Cryptography", we contrast a few segments of the plaintext and the segments of the code message however in breaking "Steganography" we contrast the cover object and the stego object in addition to some potential segments of the message.
7. "Cryptography" bombs when an interloper accesses the substance of the code material yet "Steganography" flops just when a pernicious client distinguishes the presence of the restricted information.

III. HSI MODEL

HSI represents "Hue, Saturation, and Intensity". At the point when people see a shading object it is portrayed by its tone, immersion, and brilliance. Tone is a shading characteristic that portrays unadulterated shading ("yellow", "orange", or "red"). Immersion gives a proportion of how much unadulterated shading is weakened by white light. Brilliance relies on shading power, which is key factor in depicting shading sensation. The power is effectively quantifiable and the outcomes are likewise effectively interpretable. In this way the model that is utilized to depict a shading object is the "HSI model". The "HSI model" decouples the power from shading conveying data (tint and immersion) in a shading picture.

IV. PROPOSED ALGORITHM

All the conveying bodies need the classification, trustworthiness and credibility of their privileged Intel. Various methodologies are utilized to adapt to these security issues like computerized declaration, advanced mark and "Cryptography". However, these strategies alone can't be compromised. "Steganography" is the best answer for these issues as it shrouds the presence of privileged information. This paper proposes a novel picture "Steganography" "LSB" based procedure for "RGB" pictures utilizing shading space trading from "RGB" to "HIS". The restricted information is implanted in "I-Plane" of "HIS" shading model utilizing "LSB" technique. At last the resultant picture is retransformed to "RGB" shading model to make the stego picture.

V. SHADING MODELS

Shading models are otherwise called shading frameworks or shading spaces. The primary objective of these shading spaces is to address all tones in a standard manner. A shading model is a method of addressing a bunch of tones numerically. The most well known shading spaces are "RGB", "YCbCr (Luminance Component, Chroma Blue distinction, Chroma Red contrast)" and "CMYK (Cyan, Magenta, Yellow and Black)", "HSI (Hue, Saturation and Intensity)". The "HIS" shading model is gotten from "RGB" shading space that addresses colors the manner in which the natural eyes see and decipher colors. Natural eye portrays colors by its tone, immersion and force. Shade addresses an unadulterated shading for example unadulterated red, yellow and so forth Immersion gives us a proportion of how much unadulterated shading is weakened by white light. Power is the brilliance of shading.

VI. NECESSITY OF "HSI SHADING MODEL" FOR EMBEDDING

The proposed technique utilizes "HIS" shading space for data stowing away on account of the accompanying reasons.

- Processing a picture in "RGB" shading framework is generally more troublesome and tedious. Every one of the three upsides of a specific pixel should be perused, the force is then determined, the ideal changes is made, new "RGB" esteems are recalculated and put away.
- The brilliance data in "RGB" shading space is implanted in its each layer which demonstrates that every one of the three layers are emphatically associated to each other and any progressions to one of its layer will have its comparing impact on different layers.
- To create a specific tone in "RGB" shading space, every one of the three parts should be of equivalent data transmissions.
- "RGB" is certainly not a productive shading space when we are worried about genuine pictures.
- To basically preparing, programming and end client controls.

VII. EMBEDDING ALGORITHM

Information: Cover Color Image, Secret information
Yield: Stego Image

- Stage 1: Take the cover "RGB" picture and privileged information.
- Stage 2: Convert the "RGB" picture into "HIS" shading model utilizing area 3.1.2 equations.
- Stage 3: Convert the privileged information into "1-D" exhibit of pieces.
- Stage 4: Take a pixel from "I-Plane" and supplant its "LSB" with a mysterious bit.
- Stage 5: Repeat Step 4 until and except if all mysterious pieces are encoded in the "I-Plane" pixels.
- Stage 6: Convert the "HIS" picture into "RGB" shading space utilizing the formulae of area 3.1.3.
- Stage 7: Write the stego picture.

VIII. EXTRACTION ALGORITHM

Information: Stego Image
Yield: Secret information

- Stage 1: Take the stego picture and convert it into "HIS" shading space.
- Stage 2: Consider the "I-Plane" just for extraction of restricted information.
- Stage 3: Extract the "LSB" of current pixel from "I-Plane" of "HIS" picture.
- Stage 4: Repeat Step 3 until and except if all mysterious pieces are decoded.
- Stage 5: Convert secret pieces into privileged information for example text, picture and so on.

.

IX. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed strategy, “LSB” procedure is mimicked utilizing “MATLAB R2013a”. For tests we have installed variable measure of code in various standard shading pictures of same and various measurements to assess the exhibition of the proposed strategy. The proposed procedure is assessed by 3 alternate points of view; concealing similar measure of code in various pictures of similar measurements; concealing variable measure of code in similar picture of similar measurement and concealing same measure of code in similar picture of various measurements. The standard shading pictures utilized for tests are “lena.png”, “baboon.png”, “peppers.png”, “trees.tiff” and so forth.

X. COMPARISON OF PROPOSED METHOD WITH EXISTING METHODS

The correlation among proposed calculation, basic “LSB” and calculation dependent on two kinds of investigation named as emotional examination and target examination is finished. Abstract examination is finished utilizing “Human Visual System (HVS)” to see the progressions between the cover and stego pictures and their comparing histograms.

XI. CONCLUSION

This paper proposed a novel methodology of picture “Steganography” for real nature pictures with better indistinctness, security and power. The said approach utilizes the “HIS” shading model to conceal secret messages inside shading pictures to build the security of the proposed procedure. A normal “PSNR of 75.57Db” is accomplished with this original methodology which shows the superioty of the proposed strategy when contrasted with existing techniques. This strategy presents and adds an additional security level boundary in the method of an aggressor which makes the assault on this calculation horrendous and misleads the course of steganalysis.

REFERENCES

1. Z. Jan, F. Jabeen, A. Jaffar, and A. Rauf, "Watermarking scheme based on wavelet transform, genetic programming and Watson perceptual distortion control model for JPEG2000," in *Emerging Technologies (ICET), 2010 6th International Conference on*, 2010, pp. 128-133.
2. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image “Steganography”: Survey and analysis of current methods," *Signal processing*, vol. 90, pp. 727-752, 2010.
3. S. Thenmozhi and M. Chandrasekaran, "A novel technique for image “Steganography” using nonlinear chaotic map," in *Intelligent systems and control (ISCO), 2013 7th international conference on*, 2013, pp. 307-311.
4. M. Karim, "A new approach for LSB based image “Steganography” using secret key," in *14th International Conference on Computer and Information Technology (ICCIT 2011)*, 2011, pp. 286-291.
5. E. A. Silva, K. Panetta, and S. S. Agaian, "Quantifying image similarity using measure of enhancement by entropy," in *Defense and Security Symposium*, 2007, pp. 65790U-65790U-12.
6. A. Mittal, R. Soundararajan, and A. C. Bovik, "Making a “completely blind” image quality analyzer," *Signal Processing Letters, IEEE*, vol. 20, pp. 209-212, 2013.