Image Steganography Using Texture Synthesis Process

N. M. Maske[1], P. R. Gadekar[2], R. S. Jamgekar[3]
[1,2,3]*Department of Computer Science & Engg, Solapur University, Solapur*
SKN Sinhgad College of Engineering, Korti, Solapur, MS, India
[1]maske.nitinraj@gmail.com, [2]gadekar.prakash@gmail.com, [3]rs.jamgekar@gmail.com

Abstract- A steganography is a specialty of concealing secret information into computerized media, for example, picture, sound, video and so on. Here we are going to join the work of steganography alongside picture preparing. To do this a composition union procedure is utilized which re-tests information surface picture to make another surface union image Existing steganography procedure is much costly and not all that strong in light of the fact that if the extent of the secret message expands it results into contortion of the picture. A composition union procedure gives implanting limit so that to shroud the vast message. With the surface combination handle the clear picture is built from information picture and the data picture is isolated into no. of various patches. These patches are given a patch ID and arbitrarily stuck on the clear picture. To do this, the list table is developed which gives a section to every patch. The record table is developed by utilizing a secret key so that the individual having a secret key can just get to the list table. Record table advises where to glue the patch on the clear picture. The message is partitioned into byte and put away into byte exhibit. Each of the byte is then chosen and put away into chose patch and is glued onto clear picture.

Keywords—Data embedding, example-based approach, reversible, steganography, texture synthesis.

I. INTRODUCTION

The steganography is a specialty of concealing presence of the information in another transmission medium to accomplish the secret correspondence. It is not the swap for the cryptography yet rather it helps the security. Steganography technique utilized as a part of this undertaking is based on reversible composition amalgamation process. In the common steganography process two gatherings attempt to make secure correspondence and whose achievement relies on upon recognizing the presence of the correspondence and whose achievement relies on upon correspondence and whose achievement relies on upon recognizing the presence of the correspondence. In addition a steganography is a component which disguises the secret messages inside other perfect media so that any foe couldn't have the capacity to identify it. There are different steganographic calculations accessible inthe writing whichprovides highamount of security with lower contortion. Be that as it may, these calculations are entirely brutal to execute as they neglect to give heartiness. In this undertaking surface blend procedure is generally utilized which takes source composition picture as a data and makes the new stego integrated picture as a yield. The stego manufactured picture is a piece of secret message and additionally the source surface picture.

This methodology has three principle points of interest.

1. Preliminary procedure of orchestrating the surface picture of an arbitory size can offer an ideal installing limit which is relative to the span of stego organized picture.
2. As the stegotextured picture is made out of source composition, our proposed framework is not helpless against any sort of dangers created in steganalytic calculation.
3. Most vitally, a proposed framework can acquire different functionalities to return the source surface back.

With above focal points, the proposed framework will be undeniable to combine source composition picture and force security over it by installing the secret message over to it. This summary is sorted out as takes after.

II. BACKGROUND

A customary steganographic application joins in disguise correspondences between two social events whose vicinity is dark to a possible attacker and whose accomplishment depends on after recognizing the vicinity of this correspondence Most picture steganographic calculation get a present picture as a spread medium. The expense of embedding secret messages into this spread picture is the picture curving experienced in the stego image. In late work, the pixel based methodology is utilized.

In the pixel based methodology, first the clear picture is developed from the given info picture and the secret message to cover is encoded onto that clear picture by gleaming suitable pixels. Remaining pixels are covered as it depends on the data picture. With this method we can conceal the information upto vast degree. The limit gave by the technique relies on upon the quantity of the specked examples.

III. LITERATURE REVIEW

Paper title: Hide and seek: an introduction to steganography
Author:N. Provos and P. Honeyman
Year:2003

Steganography is the workmanship and investigation of composing shrouded messages in a manner that nobody, aside from the sender and expected beneficiary, associates the presence with the message, a type of security through lack of clarity. The word steganography is of Greek word which signifies "disguised composition" from the Greek words Stefano's signifying "secured or ensured", and graphic signifying "writing". Search [7].

Paper title : A high-capacity steganographicapproachfor 3D polygonal meshes
Author:Y.-M. Cheng and C.-M.Wang
Year: 2006
In PC based steganography, pictures, sound records, reports, and even three-dimensional (3D) models might all serve as harmless searching hosts for secret messages. With the improvement of various3D applications and PC activity, numerous steganography and watermarking plans have been introduced for 3D models. This paper shows a high-limit steganographic approach for 3Dpolygonal cross sections. This strategy first uses an altered multi-level implant procedure (MMLEP) that canembed no less than three bits for every vertex with minimal visual bending. Moreover, another representation revamp procedure(RRP) in view of the representation area to accomplish the higher limit with no visual bending. itself [5].
Paper title: Texture synthesis by non-parametric sampling
Author: A Efros and T. K. Leung
Year: 1999
In the pixel based composition union procedure , we first build clear picture from the given data picture. The clear picture will go about as a workbench where we conceal the secret message. In this procedure the secret message to stow away is initially encoded by sparkling a portion of the pixels of clear picture, whatever remains of the pixels are covered on that clear picture in light of the data picture .[9]
Paper title: Fast texture synthesis using tree-structured vector quantization
Author: L.-Y. Wei and M. Levoy
Year: 2000
This paper give accentuation on concealing the information utilizing LSB calculation. The LSB remains for Least Significant Bit calculation. In this we separate the picture into no of bits and store these bits into byte exhibit. The secret message is additionally separated into bits. We take every bits of the secret message and supplant that with minimum noteworthy piece of the picture. With this methodology we can have the capacity to shroud secret data however in the event that thesize of the message is expanded then it prompts picture contortion [8].

IV. PROPOSED SYSTEM

The proposed system algorithm can provide various numbers of embedding capacities, produce a visually possible the texture images or recover the source texture. The proposed an image reversible data hiding algorithm which can recover the cover image without as any distortion from the stego image after the hidden data have been extracted. The basic unit used for our steganographic texture synthesis is referred to as the patch**.**

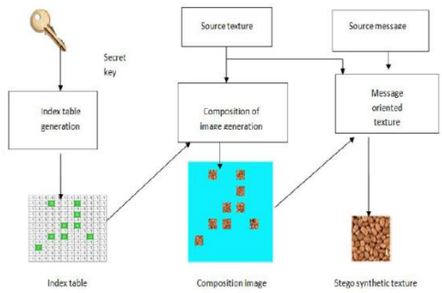


Fig.1. Architecture of proposed system

V. METHODOLOGY

The proposed steganography process uses the patch based algorithm. The image composition procedure in patch based algorithm works as follows:

- Take the input image.

We call the input image as source texture image. This image may be captured in a photograph or drawn by an artist to create synthesized texture image which is having similar appearance.

- Create the blank image from the given input image.

The purpose of creating the blank image from the input image is that the blank image is going to act as workbench where the patches will be pasted at the end.

- Divide the input image into no. of patches.

First the input image is divided into no. of patches. Each patch is having two areas:
I. Kernal boundary
II. Region boundary

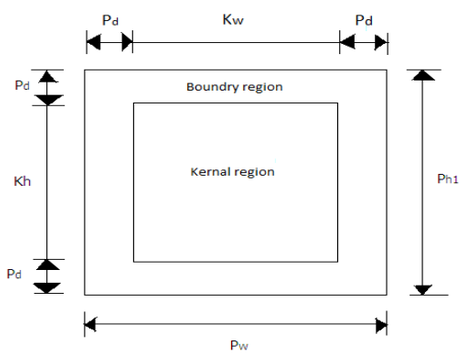


Fig 2 :- Block diagram of patch

As shown in the above figure Kw and Khrepresents the size &Pw represents the depth of patch. Store the bits of message data into separate patch and compose the image.

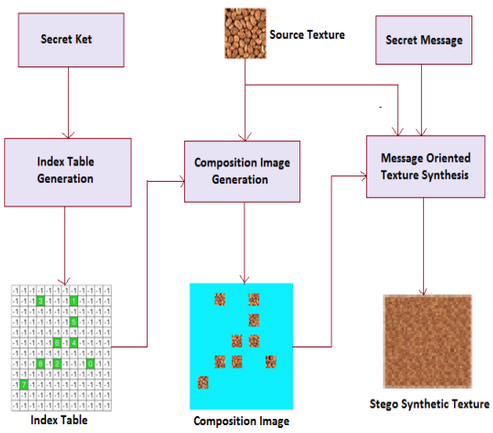


Fig 3 :- Flowchart of message embedding procedure

To develop message inserting technique, taking after steps are performed

5.1Generate the index table.

The file table stores the area data of source patch set SP in the synthetic texture. The file table permits us to get to the synthetic texture and recover the source texture totally. While producing list table we have to give the secret key to the confirmation reason.

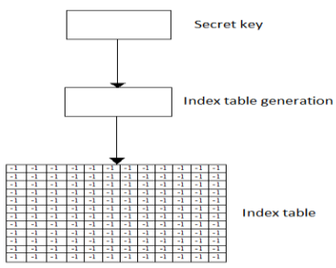


Fig 4:- Index table generation

As appeared in the figure above, at first the section in the record table is - 1 which speaks to that it is unfilled. We give the patch ID to each of the patch and afterward change the passage in the record table by the patch ID and haphazardly glue the patches onto the clear image called as workbench.

5.2 Composition image era.

In this module we build orchestrated image which is a blend of various patches. To build the integrated image, suitable hopeful patches must be chosen from the patch list. To choose the patch the record table is alluded which advises where to glue the in the clear image. The passages spoke to by green shading in list table shows the patch ID and tells the position where the patches are glued onto clear image.

As appeared in the figure of record table, the sections 1,3,5,6,4,2,0,8,7 demonstrates that these are the positions into the clear image where we have to glue the image that contains a secret message. That is the reason these passages are appeared in the green shading. The workbench demonstrates how the patches are stuck on the clear image and how it will look while building piece image system.

5.3 Message oriented texture synthesis.

In this module we make stego synthetic texture image which disguises a secret message. To develop stego synthetic image , first the message is changed over into bytes and taken as data to message oriented texture synthesis process. Alongside this source texture image and synthesis image is likewise taken asInformation to this procedure.

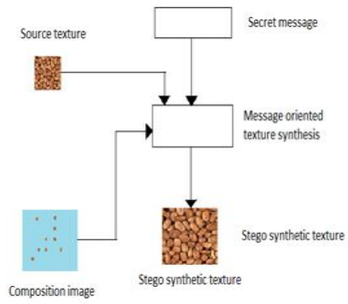


Fig 5:- Generation of stego synthetic image

The disintegration method is precisely inverse to the image structure technique. In the image deterioration technique, we are going to separate the first message from the image. To do this first the suitable patch is extricated from the made image. The patch contains a scrambled information. The extraction of patch is finished by alluding the record table. The record table tells where the patch in the image is glued and in light of this data the patch is removed from the made image. Once the patch is separated, the following assignment is to unscramble the encoded message. The message can be scrambled by utilizing any of the encryption calculation. The principle explanation for scrambling the message is to give high security to the private information. So with the encoded message regardless of the possibility that the message is scrambled by any third individual, he/she is not ready to identify the substance inside the message body unless and until they have an unscrambling key with them. The message extraction methodology can be performed in various stages as appeared in the figure of flowchart of message extraction peocedure. The flowchart of message extraction technique is given in the accompanying figure. The proposed work provides some extra facility to the user to provide more security to the system. The user that want to access the system needs to first login to the system. If he/she is already to the system then they need to enter their use id and password which is provided after the registration. If they are not registered then they need to register to the system by providing details of information to the system. Once they complete their registration the system will provide user id and password to the user which they need to enter at the time of login to the system.

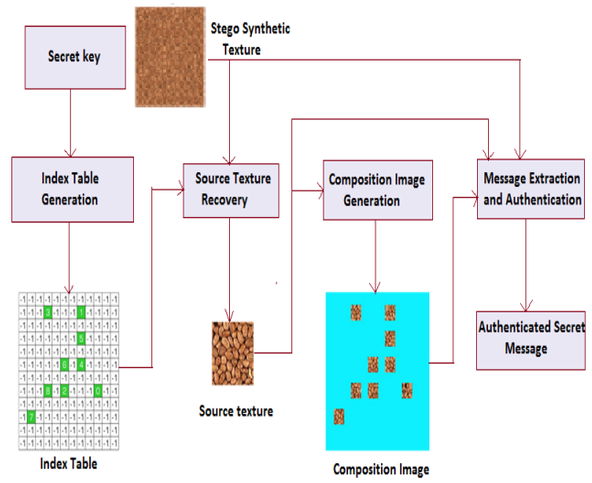
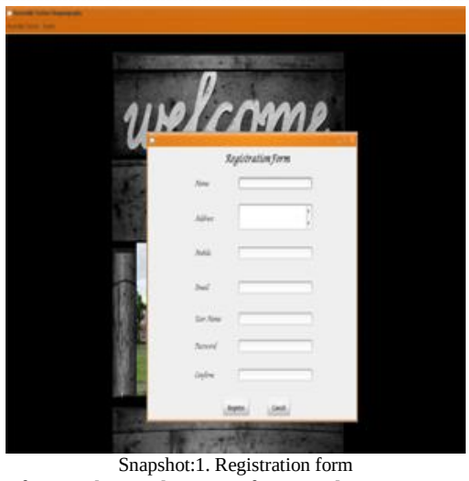


Fig 6 :- Flowchart of message extraction procedure

Above is the figure for removing the message from the image. As appeared in the figure to separate the message we initially need file table. The list table is the information structure which stores the data with respect to position of the patch inside the clear image. When it has been recognized the following assignment is source texture recuperation. The source texture is only recouping or separating the source patch from the image. Once the position of source patch is recognized the following technique is to era of piece image method. Here in this system the patches are really removed from the image by taking the reference of position from the file table. Once the patches are separated from the image, the precise next errand is to decode the encoded message. To unscramble the message, the beneficiary need the secret key with him. The measure of the secret key relies on upon the kind of encryption calculation used to scramble the message. The message can be scrambled by utilizing any of the encryption system depends senders decision. After unscrambling process, the beneficiary can get the first secret message. Here, the patch based stego synthetic texture calculation is utilized. The explanation for utilizing this calculation is to beat the downsides of LSB calculation in which the contortion rate is much higher which lessens the nature of the image. The proposed calculation takes mind that the nature of the image can not be decreased.

VI. RESULTS AND EVALUATIONS

To provide more security, user need to register to the system. After successful registration to the system, the system will provide unique username and password. The user need to enter their username and password to log in to the system. Following snapshots shows how the system works.

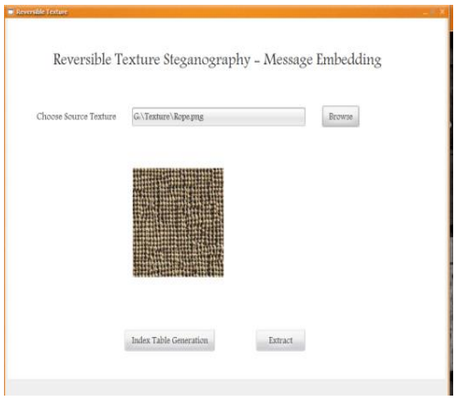


Snapshot:1. Registration form

Above figure shows that user first needs to register to the system by providing detail of information shown in the snapshot.

Snapshot:2. Login Form

Once the registration is completed the username and password is provided to the system which the user need to enter during login.



Snapshot:4. Selection of source texture

Once user login to the system the next step is selecting the source texture image.

Snapshot:4. Embedding of secret message

Snapshot 4 shows that user need to write their secret message into the textbox and then embed that secret message into source texture.

Snapshot:4. Extracting Message

When user want to extract the message from the source texture user first needed to select the source texture where the secret message is hidden inside.

VII. FUTURE SCOPE

Average image steganography process decreases the image quality as though the extent of secret message is sufficiently vast .So in the current steganography system it is normal that the span of the information must match the measure of the image. On the off chance that the size surpasses, it prompts image contortion. Our proposed approach gives brilliant image regardless of the fact that the measure of the secret message is much huge and diminishes the image processing Methodology. By providing the user id and password more security is provided to the system so that only authorized person can access the system and system become more secure.

VIII. CONCLUSION

With the proposed framework we can insert the measure of the image and give amazing image which keeps away from the bending of image quality which the current framework can not..The proposed framework is a great deal more powerful against any sort of assault and give high level of security to the classified data hidden inside the image patches. The proposed framework can be consolidated with other steganographic frameworks to give high level of security. With this framework the message can not be gotten to by any individual aside from the approved individual and who is having a protected key with him/her.

REFERENCES

[1] Kuo-Chen Wu and Chung-Ming Wang 'Steganography Using Reversible Texture Synthesis' IEEE Transactions on image processingvol: 24 no: 1 year 2015

[2] S.-C. Liu and W.-H.Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," IEEE Trans. Inf.Forensics Security, vol. 7, no. 5, pp.1448-1458, 2012.

[3] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," IEEE Comput.Graph. Appl., vol. 29, no. 6,pp. 74-81,2009.

[4] H. Otori and S. Kuriyama, "Data-embeddable texture synthesis," in Proc.of the 8th International Symposium on Smart Graphics, Kyoto, Japan,2007, pp. 146-157.

[5] Y.-M. Cheng and C.-M.Wang, "A high-capacity Steganographic approach for 3D polygonal meshes," The Visual Computer, vol. 22, no. 9, pp.845-855, 2006.

[6] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006

[7] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," Security &Privacy, IEEE, vol. 1, no. 3, pp. 32-44,2003

[8] L.-Y. Wei and M. Levoy, "Fast texture synthesis using tree-structured vector quantization," in Proc. of the 27th Annual Conference on Computer Graphics and Interactive Techniques,2000,pp. 479-488.

[9] A Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. of the Seventh IEEE International Conference on Computer Vision, 1999, p.103Z.