# Steganography Using Patch Based Algorithm

Nitin Maske[1], Pratik Kurzekar[2], Balkrushna Jagdale[3] & Harun Tamboli[4]

[1]*Department of Computer Science and Engineering, SVERI's College Of Engineering, Pandharpur*

[2]*Department of Computer Science and Engineering, SVERI's College Of Engineering, Pandharpur*

[3]*Department of Computer Science and Engineering, SVERI's College Of Engineering, Pandharpur*

[4]*Department of Computer Science and Engineering, SVERI's College Of Engineering, Pandharpur*

[1]*nmmaske@coe.sveri.ac.in,*

[2]*pkkurzekar@coe.sveri.ac.in,*

[3]*bbjagdale@coe.sveri.ac.in,*

[4]*hmtamboli@coe.sveri.ac.in*

***Abstract:*** *A steganography is associate degree art of concealment confidential knowledge into digital media like image, audio, video etc. Here we tend to square measure attending to mix the work of steganography in conjunction with image process. to try to to this a texture synthesis method is employed that re-samples input texture image to form a brand new texture synthesis image. Existing steganography method is way valuable and not therefore strong as a result of if the dimensions of the key message will increase it results into distortion of the image. A texture synthesis method provides embedding capability so to cover the big message. With the feel synthesis method the blank image is made from input image and therefore the input image is split into no. of various patches. These patches square measure given a patch ID and every which way glued on the blank image. To do this, the index table is made that provides associate degree entry for every patch. The index table is made by employing a secret key so the person having a secret key will solely access the index table. Index table tells wherever to stick the patch on the blank image. The message is split into computer memory unit and hold on into computer memory unit array. every of the computer memory unit is then elect and hold on into elect patch and is glued onto blank image.*

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

## 1. Introduction

The steganography is associate degree art of concealing existence of the information in another transmission medium to attain the key communication. it's not the replacement for the cryptography however rather it boosts the protection. Steganography methodology utilized in this project relies on reversible texture synthesis method. within the typical steganography method 2 parties attempt to build secure communication and whose success depends on police work the existence of the communication and whose success depends on communication and whose success depends on police work the existence of the communication. furthermore a steganography may be a mechanism that conceals the key messages within different compatible media so any enemy couldn't be ready to find it. There area unit numerous steganographic algorithms on the market within the literature that provides high quantity of security with lower distortion. however these algorithms area unit quite harsh to implement as they fail to produce lustiness. during this project texture synthesis method is wide used that takes supply texture image as associate degree input associate degreed creates the new stego synthesized image as an output. The stego artificial image may be a composition of secret message likewise because the supply texture image.

**This approach have 3 main advantages.**

1. Preliminary method of synthesizing the feel image of associate degree arbitory size offers associate degree optimal embedding capability that is proportional to the dimensions of stego structured image.

2. Because the stegotexctured image consists of supply texture, our planned system isn't vulnerable to any quite hazards generated in steganalytic formula.

Most significantly, a planned system will inherit numerous functionalities to revert the source texture back. With higher than blessings, the planned systems are going to be full-fledged to synthesize supply texture image and impose security over it by embedding the key message over thereto. This outline is organized as follows. Section a pair of can give elaborate discussion concerning the background of the work. Section three can stress on the connected work before development of planned system whereas section four can give the state of art to develop the corresponding system. Scope and objective behind the planned system area unit laid out in section five, six severally whereas section seven goes on elaborating the implementation facet of our system. Finally section eight concludes the work with conclusion.

## 2. Background

A regular steganographic application incorporates concealed correspondences between 2 gatherings whose presence is obscure to a conceivable aggressor and whose accomplishment depends on upon distinguishing the presence of this correspondence Most image steganographic algorithmic rule receive a current image as a ramification medium. The value of implanting secret messages into this cowl image is that the image twisting skilled within the stego image. In recent work, the pel based mostly approach is employed. Within the pel based mostly approach, 1st the blank image is built from the given input image and therefore the secret message to hide is encoded onto that blank image by glowing acceptable pixels. Remaining pixels square measure coated because it is predicated on the input image. With this system we are able to hide the information upto giant extent. The capability provided by the strategy depends on the quantity of the dotted patterns.

## 3. Literature Review

Steganography is that the art and science of writing hidden messages in such the simplest way that nobody, aside from the sender and meant recipient, suspects the existence of the message, a style of security through obscurity. The word steganography is of Greek word which implies "concealed writing" from the Greek words steganos that means "covered or protected", and graphei that means "writing” Search[7]. In computer-based steganography, images, audio files, documents, and even three-dimensional (3D) models could all function innocuous-looking hosts for secret messages. With the event of various3D applications and pc animation, several steganography and watermarking schemes are conferred for 3D models. This paper presents a high-capacity steganographic approach for 3Dpolygonal meshes. This technique initial uses a changed multi-level imbed procedure (MMLEP) that may imbed a minimum of 3 bits per vertex with very little visual distortion. Moreover, a brand new illustration arrangement procedure (RRP) supported the representation domain to attain the upper capability with no visual distortion itself[5]. within the element based mostly texture synthesis method, we tend to initial construct blank image from the given input image. The blank image can act as a bench wherever we tend to hide the key message. during this method the key message to cover is initial encoded by glowing a number of the pixels of blank image, the remainder of the pixels area unit coated on it blank image supported the input image.[9] This paper provide stress on activity the info mistreatment LSB algorithmic rule. The LSB stands for least vital Bit algorithmic rule. During this we tend to divide the image into no of bits and store these bits into computer memory unit array. The key message is additionally divided into bits. we tend to take every bits of the key message and replace that with least vital little bit of the image. With this approach we are able to hide secret info however if the dimensions of the message is magnified then it results in image distortion [5].

## 4. Problem Statement

To create synthesized stego texture image that conceals secret message, concealing reborn bytes of secret message into the image patches by choosing applicable candidate patch from the list of patches then paste it onto a blank image.

## 5. Objective

Following area unit the modules to be developed:
1. **Index table generation:** Index table contains AN entry for every patch and tells wherever to stick the patch onto the blank image.

2. **Composition image generation:** Image consists of multiple patches. we have a tendency to choose applicable candidate patches and paste it onto blank image therefore to form synthesized image that is composition of multiple patches.

3. **Message bound texture synthesis:** during this module initial we have a tendency to convert the key message into computer memory units and store it into byte array then we have a tendency to take these bytes, supply texture and composed image along to form stego synthesized texture image.

4. **Stego artificial texture:** Finally we have a tendency to get the stego synthesized image that conceals secret message

## 6. Scope

Typical image steganography method reduces the image quality as if the scale of secret message is giant enough .So within the existing steganography technique it's expected that the scale of the information should match the scale of the image. If the scale exceeds, it results in image distortion. Our planned approach provides top quality image even though the scale of the key message is far giant and reduces the image distortion.

## 7. Methodology

The planned steganography method uses the patch primarily based algorithmic program. The image composition procedure in patch primarily based algorithmic program works as follows:

1. **Take the input image.**
We decision the input image as supply texture image. This image could also be captured associate degree exceedingly in a very photograph or drawn by an creative person to form synthesized texture image that has similar look.

2. **Produce the blank image from the given input image.**

The purpose of making the blank image from the input image is that the blank image goes to act as bench wherever the patches are going to be glued at the tip.

3. **Divide the input image into no. of patches.**
First the input image is split into no. of patches. every patch has 2 areas:
I. Kernal boundary
II. .Region boundary

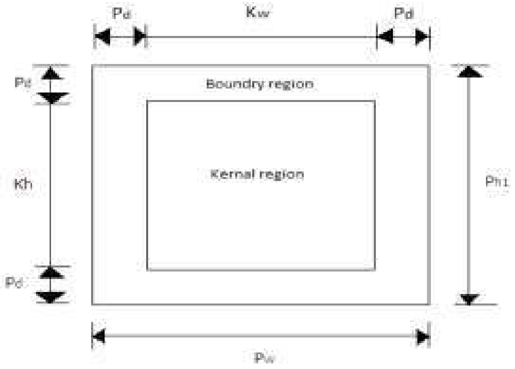


Fig 1 :- Block diagram of patch [1]

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

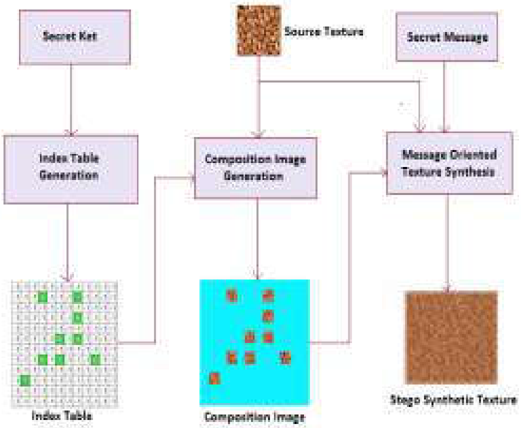
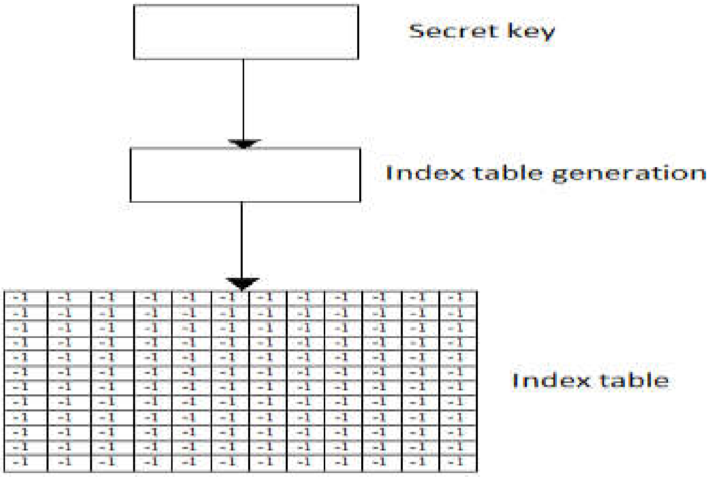


Fig 2 :- Flowchart of message embedding procedure

To construct message embedding procedure, following steps are performed

**1. Generate the index table.**
The index table stores the placement info of supply patch set SP within the artificial texture. The index table permits US to access the artificial texture and retrieve the supply texture fully. whereas generating index table we want to supply the key key for the authentication purpose. we tend to initial confirm the size of the index table (Tpw×Tph). Given the parameters Tw and Th, that area unit the breadth and also the height of the artificial texture we tend to will synthesize, the amount of entries during this index table may be determined victimisation (3) wherever feeding denotes the amount of patches

within the stegosynthetic texture. For simplicity, we tend to selected acceptable parameters for Tw, Th, Pw, Ph, and Pd, in order that the amount of entries is Associate in Nursing number. As Associate in Nursing example, if Tw×Th=488×488,Pw×Ph=48×48, and Pd=8, then we are able to manufacture Associate in Nursing index table (12×12) containing one hundred forty four passages. once we convey supply texture to accomplish the means of changeableness, the supply patches may be disseminated in an exceedingly fairly scanty means if the artificial texture incorporates a determination that's a lot of larger than that of the supply texture. Unexpectedly, the supply patches can be sent in an exceedingly fairly thick means if the artificial texture incorporates a determination that's somewhat larger than that of the supply texture. For the patch conveyance, we tend to abstain from situating a supply texture patch on the outskirts of the artificial texture. this may urge the outskirts to be created by message-oriented texture synthesis, rising the image nature of the artificial texture. Once the placement info is set, we've to put in writing the encrypted secret message into the patch. to try to to this the suitable patch should be selected . This choice relies on the entry into the index table that tells that patch to pick out and wherever to stick the patch into the blank image.



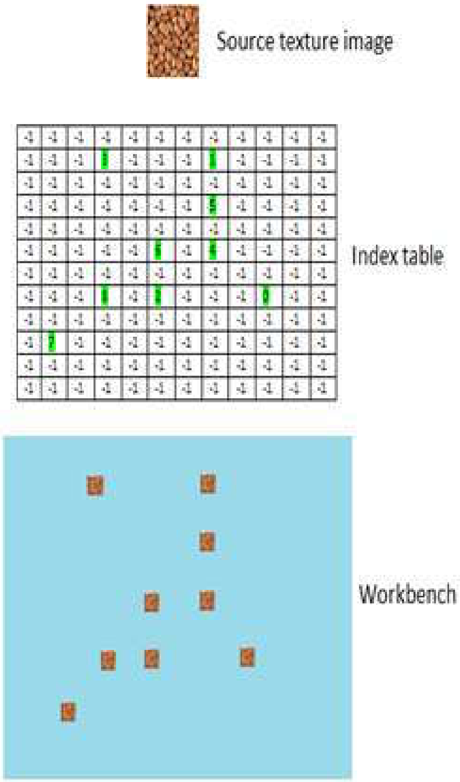
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |

**Fig 3:- Index table generation**

As shown in the figure above, initially the entry in the index table is -1 which represents that it is empty. We provide the patch ID to each of the patch and then change the entry in the index table by the patch ID and randomly paste the patches onto the blank image called as workbench.

**2. Composition image generation.**

In this module we tend to construct synthesized image that may be a combination of various patches. To construct the synthesized image, acceptable candidate patches should be selected from the patch list. to pick the patch the index table is referred that tells wherever to stick the within the blank image. The entries depicted by inexperienced colorise index table indicates the patch ID and tells the position wherever the patches area unit glued onto blank image. As shown within the figure of index table, the entries one,3,5,6,4,2,0,8,7 indicates that these area unit the positions into the blank image wherever we want to stick the image that contains a secret message. that's why these entries area unit shown within the inexperienced color. The work table shows however the patches area unit glued on the blank image and the way it'll look whereas constructing composition image procedure.



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | 3 | -1 | -1 | -1 | 1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | 5 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | 6 | -1 | 4 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | 8 | -1 | 2 | -1 | -1 | -1 | 0 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | 7 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |

**Fig 4:- Illustration of composition image**

### 3. Message oriented texture synthesis.

In this module we have a tendency to produce stego artificial texture image that conceals a secret message. To construct stego artificial image, initial the message is regenerate into bytes and brought as input to message destined texture synthesis method. beside this supply texture image and composition image is additionally taken as input to the present method.

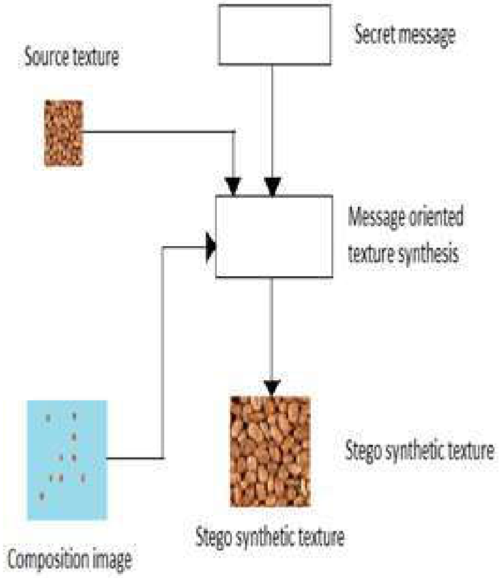


**Fig 5:- Generation of stego synthetic image**

The image decomposition procedure in patch based algorithm works as follows:

The decomposition procedure is exactly opposite to the image composition procedure. In the image decomposition procedure, we are going to extract the original message from the image. To do this first the appropriate patch is extracted from the composed image. The patch contains a encrypted data. The extraction of patch is done by referring the index table. The index table tells where the patch in the image is pasted and based on this information the patch is extracted from the composed image. Once the patch is extracted, the next task is to decrypt the encrypted message. The message can be encrypted by using any of the encryption algorithm. The main reason behind encrypting the message is to provide high security to the confidential data. So with the encrypted message even if the message is encrypted by any third person, he/she is not able to detect the contents inside the message body unless and until they have a decryption key with them. The message extraction procedure can be performed in different phases as shown in the figure of flowchart of message extraction procedure.

## 8. Conclusion

With the proposed system we are able to introduce the dimensions of the image and supply prime quality image that avoids the distortion of image quality that the present system cannot. The planned system is way additional strong against any quite attack and supply high degree of security to the confidential knowledge hidden within the image patches. The planned system may be combined with alternative steganographic systems to produce high degree of security. With this method the message can't be accessed by someone except the approved person and WHO has a secure key with him/her.

## REFERENCES

[1] *Kuo-Chen Wu and Chung-Ming Wang „Steganography Using Reversible Texture Synthesis,, IEEE Transactions on image*

[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 VisualComputer, 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.*