A Reversible surface texture synthesis process based steganography for large data embedding

[1]Deepak S Uplaonkar, [2]Manik A Raichurakar
[1&2]Assistant Professor
[1&2]Department of Computer Engineering,
[1&2]JSPM, Narhe Technical Campus, Pune, India

Abstract : The steganography is a specialty of concealing the presence of the information in another transmission medium to accomplish the confidential communication. It is not the substitute for the cryptography yet rather it helps the security. Steganography strategy utilized as a part of this system depends on reversible surface texture synthesis process. In the average steganography process people on two sides endeavour to make secure communication and whose achievement relies upon recognizing the presence of the communication. Existing steganography process is not efficient in terms of cost and size. Increase in the size of a message may lead to distortion of the image. A novel surface texture synthesis process enables to embed and conceal large size secret messages in the stego image. With the surface texture synthesis process the clear image is built from an input image and the image is split into the number of various patches. These patches are given a fixed ID and pasted randomly on the clear image. This provides high efficiency for embedding secure data, as the size of the cover image is dependent on the size of the secret message, which will allow storing large size information or message. This system can embed the large size secret message in the image and provide the high quality image which avoids the distortion of image quality.

IndexTerms **-Data embedding, steganography, surface texture synthesis, secret messages.**

I. INTRODUCTION

Steganography is a very ancient technique which can be traced way back in 440 and has been widely used for centuries. Since inception, steganography has been employed in the physical communication like hidden messages on messenger's body, hidden messages on a paper written in secret inks, microdots were embedded in the paper and covered with an adhesive during World War II [1] and many others. Personal computers were commercialized during early 1980's. By the year 1985 [1], as personal computers were already being used for sharing information digital steganography was introduced for secure communication.

The steganography is a specialty of concealing presence of the information in another transmission medium to accomplish the confidential communication. Steganography strategy utilized as a part of this system depends on reversible surface texture synthesis process. In the average steganography process people on two sides endeavour to make secure communication and whose achievement relies upon recognizing the presence of the communication. There are numerous steganographic algorithms ready to use within the literature that provides high security with lower distortion. However these algorithms are not feasible to implement as they fail to produce resilient output.

II. LITERATURE REVIEW

Prasad Tanaji Satpute and Deipali Gore [1] had presented a technique for steganography using reversible texture synthesis stands on edge adaptive and tree-based parity check to improve the embedding capacity. One of the major limitations is that following the whole procedure there might be some exemplary in which, a chance of using same data multiple times.

Kuo-Chen Wu and Chung-Ming Wang [2] author had presented a technique of Steganography using Reversible Texture Synthesis process. This system uses patch based approach in which the secret message is made hidden.

Provos and P. Honeyman [3] author has presented an overview of steganography. Steganography is nothing but hiding the confidential data into digital media such as image, audio, video It only emphasis on working of steganography. Does not give idea about how reversible texture synthesis works.

Y.-M. Cheng and C.-M. Wang [4] In this a high-capacity steganographic approach for 3D polygonal meshes. This method uses a modified multi-level embed procedure that can embed at least three bits per vertex with little visual distortion. Image distortion rate is high.

A. A. Efros and T. K. Leung [5] This paper elaborates working of pixel based approach. In the pixel based approach hiding of confidential message is done by encoding the message into the pixels. Each output pixel is determined by the already synthesized pixels, any wrongly synthesized pixels cause propagation of errors.

S.C. Liu and W.H. Tsai [6] This paper elaborates steganography using LSB algorithm. In this approach Least Significant Bit of the image is replaced with bit of the message. With this approach if size of the message is large then it leads to image distortion.

III. METHODOLOGY

Thetemplateisusedtoformatyourpaperandstylethetext.Allmargins,columnwidths,linespaces,andtextfontsareprescribed;pleasedonotalterthem.Youmaynotepeculiarities.Forexample,theheadmargininthistemplatemeasuresproportionatelymorethaniscustomary.Thismeasurementandothersaredeliberate,usingspecificationsthatanticipateyourpaperasonepartoftheentireproceedings,andnotasanindependentdocument.Pleasedonotreviseanyofthecurrentdesignations.

In the available stegenographic methods the quality of stego image is on stakes due to the size the secret message. As, the size of secret message increases the stego image is distorted. To conquer the issue of distortion of the stego image a novel surface texture synthesis process is engaged to embed and conceal large size secret messages.

The proposed system the novel surface texture synthesis process the clear image is built from input image and the image is split into number of various patches. These patches are given a fix ID and pasted randomly on the clear image.

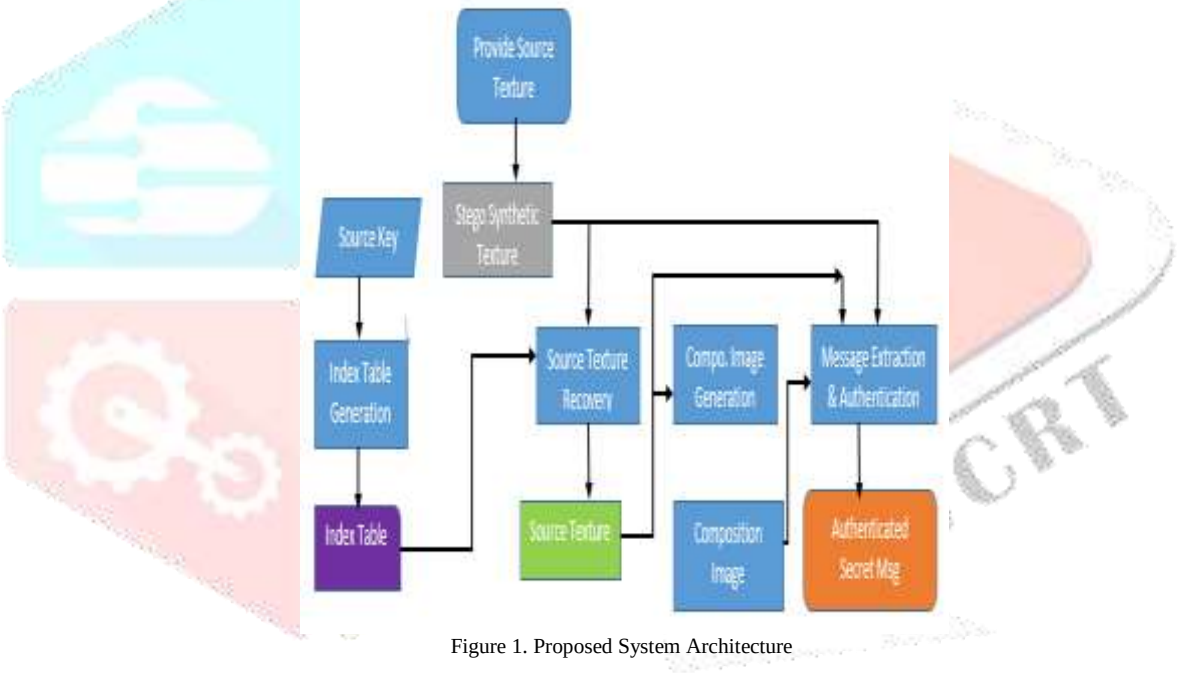

Figure 1. Proposed System Architecture

The large number of image steganography algorithms have been investigate with the increasing popularity and use of digital images.

A. Source Patch Generation

1. Size (Patch) = (Pw) *(Ph)

   Where (Pw) is width of patch and (Ph) is height.
2. Size (Kernel) = Kw×Kh,

   Where Kw and Kh is width and height of kernel region.
3. Source Texture T= Sw×Sh
4. Divide T into non overlapping kernel block of size Kw×Kh

||KB||= {kb0, kb1… kb1n}.

V. SP={spi| i = 0 to ||SP||-1}.

Where SP -source patches.
Vi. Source Patches required is,
SPn= Sw/ Kw* Sh/ Kh.

B. Index Table Generation

1. Dimension Of Index Table is given as (Tpw×Tph)
2. Total Number Of patches can be calculated as

3. $$TPn = T_{Pw} \times T_{ph} = \left\lfloor \frac{(T_w - P_w)}{(P_w - P_d)} + 1 \right\rfloor \times \left\lfloor \frac{(T_h - P_h)}{(P_h - P_h)} + 1 \right\rfloor$$

4. Select Patch priority L1 with high priority and L2 with low priority.

5. Patch Priority can be Decided Using following formula:

$$\|L1\| = \left\lceil \frac{T_{pw-2}}{2} \right\rceil \times \left\lceil \frac{T_{ph-2}}{2} \right\rceil$$

$$\|L2\| = \left\lceil \frac{T_{pw-2}}{2} \right\rceil \times \left\lceil \frac{T_{ph-2}}{2} \right\rceil$$

IV. Results and Discussion

Beforeyoubegintoformatyourpaper,firstwriteandsavethecontentasaseparatetextfile.Keepyourtextandgraphicfilesseparateuntilafterthetexthasbeenformattedandstyled.Donotusehardtabs,andlimituseofhardreturnstoonlyonereturnattheendofaparagraph.Donotaddanykindofpaginationanywhereinthepaper.Donotnumbertextheads—thetemplatewilldothatforyou.

Finally,completecontentandorganizationaleditingbeforeformatting.Pleasetakenoteofthefollowingitemswhenproofreadingspellingandgrammar.

To demonstrate the adequacy of proposed framework a few trials are directed on java based windows machine utilizing Eclipse as IDE. Mean Absolute Error (MAE) metric is generally utilized to quantify the suggestion nature of synergistic sifting techniques. Where ri,j means the normal course j in client suggestion choicer i, ri,j signifies the recommendation values, and N signifies the quantity of recommended values. Since various recommendation properties of courses have diverse value ranges, we utilize the Normalized Mean Absolute Error (NMAE) metric to gauge the proposal nature of our half and half shared sifting strategy. We characterize our NMAE to be the standard MAE standardized by the mean of the normal recommended values as takes after.

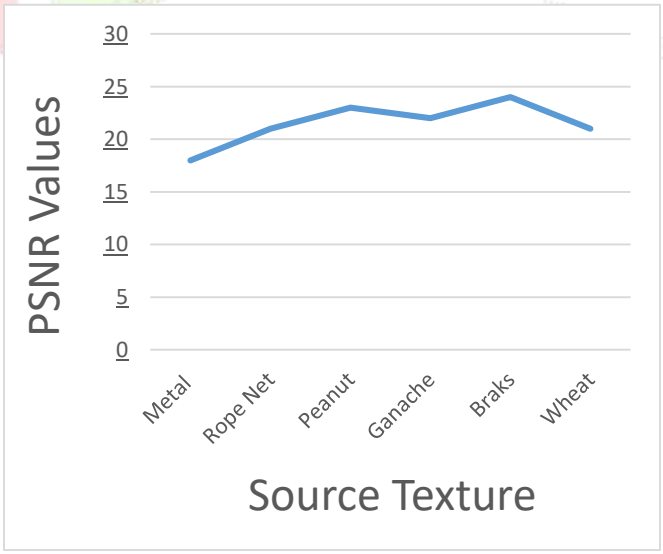

Figure 2. Existing System Result Analysis

This proportion is regularly utilized as a quality estimation between the first and a compacted picture. The higher the PSNR, the better the nature of the packed, or recreated picture. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to think about picture compressed quality. The MSE speaks to the total squared error between the compacted and the source picture, while PSNR speaks to a measure of the peak error. The lower the estimation of MSE, the lower the error. To calculate the PSNR, the component initially computes the mean-squared error utilizing the accompanying equation:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

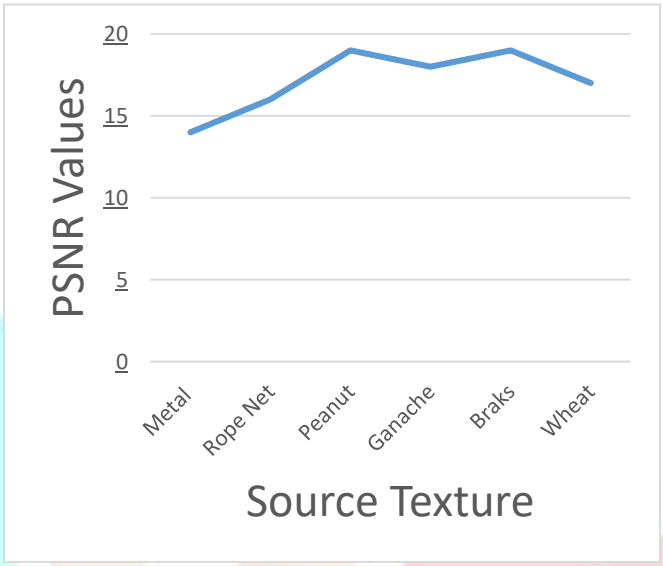

Figure 3. Proposed System Result Analysis

Where, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

Where, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc. The analysis show that the minimum PSNR value texture having minimum pixels distortion. Result analysis shows that metal texture is best to use as a stego texture.

V. CONCLUSION

Proposed system we are able to embed the scale of the image and image with high quality is provided which avoids the distortion of image quality which cannot be done through existing techniques. The proposed system is far a lot resilient against any attack and deliver high degree of security to the confidential information hidden within the image patches. The proposed system often combined with alternative steganographic systems to deliver high degree of security. With this method the message cannot be accessed by any individual except the intended user of the system.

REFERENCES

[1] Prasad Tanaji Satpute and Deipali Gore,"Image Quilting in Steganography using Reversible Texture rmation", International Research Journal of Engineering and Technology(IRJET)e-ISSN: 2395-0056 Volume:04 Issue: 07 July-2017.
[2] Kuo-Chen Wu and Chung-Ming Wang "Steganography Using Reversible Texture Synthesis", IEEE Transactions on image processing vol: 24 no: 1 year 2015.
[3] 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.
[4] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications", IEEE Comput. Graph. Appl., vol. 29, no. 6, pp. 74-81,2009.
[5] 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.

[6] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approachfor 3D polygonal meshes", The Visual Computer, vol. 22, no. 9, pp.845-855, 2006.
[7] 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.
[8] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography", Security & Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.
[9] 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.