International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 6, Nov-Dec-2018, ISSN (Online): 2395-566X

Image Stenography Using Reversible Texture Synthesis

M.Tech.Scholar Sheshank Porwal
Dept of Computer Science & Engg.
Eshan College of Engineering
Agra, India
porwalsheshank@gmail.com

Asst. Prof. Ajit Saxena
Dept of Computer Science & Engg.
Eshan College of Engineering
Agra, India

Abstract- **Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication-to hide the existence of a message from a third party. This paper is intended as a high-level technical introduction to stegano graphy for those unfamiliar with the field. It is directed at forensic computer examiners who need a practical understanding of stegano graphy without delving into the mathematics, although references are provided to some of the ongoing research for the person who needs or wants additional detail. Although this paper provides a historical context for steganography, the emphasis is on digital applications, focusing on hiding information in online image or audio files. Examples of software tools that employ steganography to hide data inside of other files as well as software to detect such hidden files will also be presented.**

Keywords:- **Steganography, cryptography, hidden writing etc.**

I. INTRODUCTION

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication.

Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing (Bauer 2002). Nevertheless, this paper will treat steganography as a separate field.

Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies and terrorists. Microdots and microfilm, a staple of war and spy movies, came about after the invention of photography (Arnold et al. 2003; Johnson et al. 2001; Kahn 1996; Wayner 2002).

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary:
steganography_medium = hidden message + carrier + steganography_key

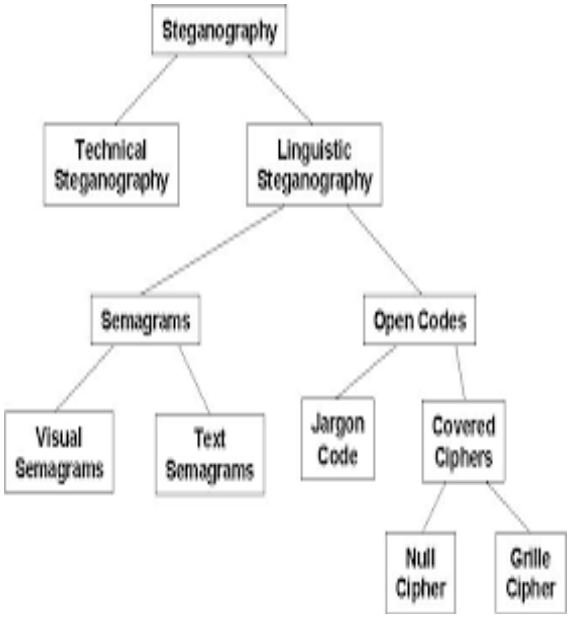

Fig.1 shows a common taxonomy of steganographic techniques (Arnold et al. 2003; Bauer 2002).

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.

- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.
- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

  As an increasing amount of data is stored on computers and transmitted over networks, it is not surprising that steganography has entered the digital age. On computers and networks, steganography applications allow for someone to hide any type of binary file in any other binary file, although image and audio files are today's most common carriers.

II.EXISTING SYSTEM

Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. The most recent work has focused on texture synthesis by example, in which a source texture image is re-sampled using either pixel-based or patch-basedalgorithms produce a new synthesized texture image with similar local appearance and arbitrary size.

Otori and Kuriyama pioneered the work of combining data coding with pixel-based texture synthesis. Secret messages to be concealed are encoded into colored dotted patterns and they are directly painted on a blank image.

III. LITERATURE REVIEW

In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), [1] Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key. The order parameter of this transform.

In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., [2] implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality.

In the year of 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. [3] Investigated on Medical records are extremely sensitive patient information a multi secure and robustness of medical image based steganography scheme is proposed. This methodology provides an efficient and storage security mechanism for the protection of digital medical images. Authors proposed a viable steganography method using Integer Wavelet Transform to protect the MRI medical image into a single container image. The patient's medical diagnosis image has been taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In this case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. It has been observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms.

In the year of 2012 Thenmozhi, S. and Chandrasekaran, M., [4] presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after

embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

In the year of 2012 Das, R. and Tuithung, T. [5] proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, in order that the Stego Image becomes standalone information to the receiver. Results show that the algorithm has a high capacity and a good invisibility. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches. The satisfactory security is maintained in this research.

In the year of 2012 Hemalatha, S, Acharya, U.D. and Renuka [6] presented integer Wavelet Transform (IWT) is used to hide the key thus it is very secure and robust because no one can realize the hidden information and it cannot be lost due to noise or any signal processing operations. Result shows very good Peak Signal to Noise Ratio, which is a measure of security. In this method the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands. In the 2012 Reddy, H.S.M., Sathisha, N. and Kumari, A. [7] worked on the steganography is used to hide. Secure Steganography using Hybrid Domain Technique (SSHDT). The cover image of different formats and sizes are considered and resized to dimensions of power of 2. The Daubechies Lifting Wavelet Transforms (LWT) is applied on cover image to generate four sub bands XA, XH, XV and XD. The XD band is considered and divided into two equal blocks say upper and lower for payload embedding. The payload of different formats are considered and resized to dimensions of power of 2.

The payload is fragmented into four equal blocks. The Decision Factor Based Manipulation (DFBM) is used to scramble further steno object to improve security to the payload. Dubieties Inverse LWT (ILWT) is applied on XA, XH, XV and XD steno objects to obtain stego image in spatial domain. It has been observed that PSNR and embedding capacity of the proposed algorithm is better compared to the existing algorithm. With the rapid development of internet and wide application of multimedia technology, people can communicate the digital multimedia information such as digital image, with others conveniently over the internet. In numerous cases, image data, transmitted over a network are expected not to be browsed or processed by illegal receivers. Consequently, the security of digital image has attracted much attention recently and many different methods for image encryption have been proposed, such as [5] Optical systems are of growing interest for image encryption because of their distinct advantages of processing 2-dimensional complex data in parallel at high speed. In the past, many optical methods have been proposed in [9]. Among them the most widely used and highly successful optical encryption scheme is double random phase encoding proposed in [4]. It can be shown that if these random phases are statistically independent white noise then the encrypted image is also a stationary white noise. In some schemes [2] [3] [5], chaos based functions are used to generate random phase mask. Such as the generalization of the conventional Fourier transform [4].

IV.RESEARCH METHODOLOGY

In this paper, we propose a novel approach for steganography using reversible texture synthesis. A texture synthesis process re-samples a small texture image drawn by an artist or captured in a photograph in order to synthesize a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography concealing secret messages as well as the source texture. In particular, in contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract the secret messages and the source texture from a stego synthetic texture.

The three fundamental differences between our proposed message-oriented texture synthesis and the conventional patch based texture synthesis are described in following: The first difference is the shape of the overlapped area. During the conventional synthesis process, an L-shape overlapped area is normally used to determine the similarity of every candidate patch. In contrast, the shape of the overlapped area in our algorithm varies because we have pasted source patches into the workbench. Consequently, our algorithm needs to provide more flexibility in order to cope with a number of variable shapes formed by the overlapped area.

V. ADVANTAGES OF PROPOSED SYSTEM

- Our approach offers three advantages.
- First, since the texture synthesis can synthesize an arbitrary size of texture images, the embedding capacity which our scheme offers is proportional to the size of the steno texture image.
- Secondly, a steganalytic algorithm is not likely to defeat this steganographic approach since the stego texture image is composed of a source texture rather than by modifying the existing image contents.
- Third, the reversible capability inherited from our scheme provides functionality to recover the source texture. Since the recovered source texture is exactly the same as the original source texture, it can be employed to proceed onto the second round of secret messages for steganography if needed.

VI. STEGANOGRAPHY USING REVERSIBLE TEXTURE SYNTHESIS

The last decade many advances have been made in the area of digital media, and much concern has arisen regarding steganography for digital media. Steganography a singular method of information hiding techniques. It embeds messages into a host medium in order to conceal secret messages so as not to arouse suspicion by an eavesdropper .A typical steganographic application includes covert communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication . In general, the host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3D model , etc. A large number of image steganographic algorithms have been investigated with the increasing popularity and use of digital images.

Most image stegano graphic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the steno image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image distortion. Consequently, a compromise must be reached between the embedding capacity and the image quality which results in the limited capacity provided in any specific cover image. Recall that image steganalysis is an approach used to detect secret messages hidden in the steno image. A steno image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image.

This leads to the second drawback because it is still possible that an image stag analytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image. In this paper, we propose a novel approach for steganography using reversible texture synthesis. A texture synthesis process re-samples a small texture image drawn by an artist or captured in a photograph in order to synthesize a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography concealing secret messages as well as the source texture.

VII.CONCLUSIONS

Original source texture, our scheme can produce a large steno synthetic texture concealing secret this paper proposes a reversible steganographic algorithm using texture synthesis. Given a message. To the best of our knowledge, we are the first that can exquisitely weave the steganography into a conventional patch-based texture synthesis. Our method is novel and provides reversibility to retrieve the original source texture from the steno synthetic textures, making possible a second round of texture synthesis if needed. With the two techniques we have introduced, our algorithm can produce visually plus is blest ego synthetic textures even if the secret messages consisting of bit “0” or “1” have an uneven appearance of probabilities. The presented algorithm is secure and robust against an RS steganalysis attack. We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications. One possible future study is to expand our scheme to support other kinds of texture synthesis approaches to improve the image quality of the synthetic textures. Another possible study would be to combine other steganography approaches to increase the embedding capacities.

REFERENCES

[1]. N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” Computer, vol. 31, no. 2, pp. 26-34, 1998.
[2]. N. Provos and P. Honeyman, “Hide and seek: an introduction to steganography,” Security & Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.
[3]. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.
[4]. 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.
[5]. 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.
[6]. I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779-1790, 2014.
[7]. J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," Multi Media, IEEE, vol. 8, no. 4, pp. 22-28, 2001.
[8]. Y. Guo, G. Zhao, Z. Zhou, and M. Pietikäinen, "Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3879-3891, 2013.
[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.
[10]. A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. of the Seventh IEEE International Conference on Computer Vision, 1999, pp. 1033-1038.
[11]. C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, "Multiscale texture synthesis," ACM Trans. Graph., vol. 27, no. 3, pp. 1-8, 2008.
[12]. 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.
[13]. H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," IEEE Comput.Graph.Appl., vol. 29, no. 6, pp. 74-81, 2009.
[14]. M. F. Cohen, J. Shade, S. Hiller, and O. Deussen, "Wang Tiles for image and texture generation," ACM Trans. Graph., vol. 22, no. 3, pp. 287-294, 2003.
[15]. K. Xu, D. Cohen-Or, T. Ju, L. Liu, H. Zhang, S. Zhou, and Y. Xiong, "Feature-aligned shape texturing," ACM Trans. Graph., vol. 28, no. 5, pp. 1-7, 2009.