DOI 10.4010/2016.1649
ISSN 2321 3361 © 2016 IJESC

Research Article Volume 6 Issue No. 6

A Novel Secure Image Steganography Using Fingerprint Image Based Key in Transform Domain

Anju PS[1], Dr. Vince Paul[2]
Department of Computer Science and Engineering
Sahrdaya College of Engineering and Technology, Kodakara, Thrissur, India
anjusuru@gmail.com[1], vinceakkara@gmail.com[2]

Abstract:
Nowadays, a lot of confidential information has been send over the internet. It is necessary to find a better way to securely sent over the internet. Steganography is method to send confidential information in a different method over the internet. This paper proposes a novel steganographic method to secure the data. In this paper DCT based steganography is proposed with the support of fingerprint based key generating system. DCT based steganography gives high embedding capacity, here the embedding capacity is much more increased because of the use of synthetic texture. Fingerprint based key generation is more secure because of its uniqueness and permanence.

Index Terms: discrete cosine transform (DCT), fingerprint, steganography, texture synthesis.

I. INTRODUCTION

In the present era a large amount of information has been send over the internet. Thus most of the data are vulnerable to attack irrespective of the confidentiality of information. Importance of securing confidential information send over the internet arises at this point. There are lots of techniques for securing data have been evolved over the year. Steganography and cryptography are more popular among that. Steganography is originated from Greek and it means hidden writing. It is way of hidden communication. Malicious users are not able to know the existence of the information passing from the sender to receiver. Steganography is about to hide the confidential information in a harmless media using some technique. Cryptography on the other hand, is converting data into another form so that a particular person who is authorized, can only read that data. In the case of cryptography, a third party can easily reveal, modify the message without breaking certain security guaranteed by the cryptosystem. It is the point where important of steganography comes. Steganography hides existence of communication; no malicious users are able to attack the confidential data.

In steganography data can be hidden using different media as a cover medium, if an image is used as cover medium then the steganography is called image steganography. Most of the image steganographic technique uses existing media as a cover medium. If we try to hide more data in such media more distortion will be encountered in that media. More distortion means malicious users are able to attack easily. Also leads to less embedding capacity.

Reversible texture synthesis approach synthesizes new texture image from an existing texture image into an arbitrary size and conceals source texture image and embeds the secret message through texture synthesis. Here a randomly generated key is used to generate an index table which is used for determining the position to hide the original texture. But such keys are easy to identify by malicious users. Also message oriented texture synthesis process leads to less embedding capacity at some point.

This paper proposes a novel steganography technique using reversible texture synthesis with a different approach. This paper uses fingerprint images of authorized persons to generate random keys which are then used for hiding original texture images. Also uses DCT based message embedding procedure to ensure high message embedding capacity. Another benefit is that it uses synthesized texture to hide the message rather than modifying an existing cover image. Also, this paper offer reversible capability, which the original texture can be recovered at the receiver side without compromising the quality so that it can be used for the second round of steganography.

The rest of the paper organized as follows, in section II literature survey of steganography techniques. In section III describes proposed algorithm followed by conclusion and future work.

II. LITERATURE SURVEY

There are several surveys that have already been done in this area of this knowledge. Some of the studies are discussed in this section.

In Mamta Juneja et. al's [1] research paper a secured robust approach of information security is proposed. It presents two component based LSB (Least Significant Bit)methods for embedding secret data in the LSB's of blue components and partial green components of random pixel locations in the edges of images. An adaptive LSB based steganography is proposed for embedding data based on data available in MSB's of red, green, and blue components of randomly selected pixels across smooth areas. It is more robust as it is integrated with an Advanced Encryption Standard(AES).

In S.Shanmuga Priya et. al's [2] article the authors propose a novel method based on LSB. Data embedding is performed using a pair of pixels as a unit, where LSB of the first pixel carries one bit of information and a function to two pixel values carries another bit of information. The proposed

method shows better performance in terms of distortion and resistance against existing steganalysis. Embedding is done in the sharper edge regions using a threshold. PSNR value is compared for adaptive and non-adaptive techniques of data hiding in gray scale & color images.

In Shweta Singhal et.al's [3] paper a new image steganography scheme is proposed in the spatial domain. In the technique, one byte of blue factor of pixels of an image have been replaced with secret bits of text data, which results in better image quality. A stego key is used for security purposes.

In M.B.Ould MEDENI et.al.'s article [4], the authors propose a novel method for hiding information within the spatial domain of the gray scale image. The Pixel Value Differencing (PVD) method segments the cover image into no overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. While embedding secret data, each pixel is split into two equal parts. The number of 1's in the most significant part is counted and the secret message is embedded in the least part according to the number of corresponding bits. The proposed method is based on four-pixel differencing and LSB substitution.

In Chin-Chen Chang et.al.'s paper [5] an adaptive method is proposed. Data is hidden based on codeword grouping. A set of code words generated using palette generation algorithm is employed in index-based images. A code word grouping based steganographic scheme for index encoding images is presented. The relationship of code words is explored to group different member sub-clusters. The size of the sub-cluster determines the hiding capacity. To enhance hiding capacity sub-clusters with larger members are grouped together & sub-clusters with smaller members are grouped together. In the embedding procedure the sub-cluster to which the closest searched codeword belongs is identified, and the original encoded codeword is modified to hide secret message. The number of sub-cluster members indicates how many bits of secret message can be embedded. A set of thresholds is used to determine members of sub-cluster. Therefore choosing an adequate threshold is important. To improve security the sequence of embedding pixels is reorganized using a pseudo random generator.

In Hemalatha.S et.al's [6] paper, the authors propose a method that uses two gray scale images of size 128 x 128 that are used as secret images and embedding is done in RGB and YCbCr domains. The quality of stego images are good in RGB domain by comparing the PSNR values. The authors have used Integer Wavelet Transform (IWT) to hide secret images in the color cover image. The authors have compared the PSNR values and image quality when embedding is done in the RGB and YCbCr domains.

In another article by Hemalatha .S et. al. [7] Integer Wavelet Transform (IWT) has been suggested to hide multiple secret images and keys in a color cover image which is more efficient. The cover image is represented in the YCbCr colour space. Two keys are obtained, encrypted and hidden in the cover image using IWT.

In Keith.L. Haynes's article [8] the author studies the use of image steganography to breach an organization's physical and cyber defences. The proposed method utilizes computer vision and machine learning techniques to produce messages that are undetectable and if intercepted cannot be decrypted without key compromise. To avoid detection DWT (Discrete Wavelet Transform) is used. The goal of a computer vision system is to allow machines to analyze an image and make a decision as to the content of that image. The computer vision can be categorized as Model-Based & Appearance Based which uses example images and machine learning techniques to identify significant areas or aspects of images that are important for discrimination of objects contained within the image. Machine learning is different from human knowledge / learning. A computer has to make decision of the presence of a face based on the numbers contained in a 2D matrix. The feature is identified by using Haar feature selection. The goal is to identify the set of features that best distinguishes between images in the different classes. In the proposed method the cover image does not contain a secret message, rather the classification of the image yields the hidden message. Since the proposed algorithm utilizes ordinary unmodified images, there are no inherent indicators of covert communication taking place.

In S.Arivazhagan et. al.'s work [9] the authors propose a method that works in the transform domain and attempts to extract the secret almost as same as the embedded one, maintaining minimal changes to cover image by using techniques like median maintenance, offset & quantization. A modified approach for embedding colour images within colour images is proposed and it overcomes the limitations in embedding. Arnold Transform is applied on the secret image to increase robustness. This transformed image is then split into the three colour planes R, G, B and are subjected to DWT individually, converted to bit stream and then concatenated to be embedded in the cover image which is also subjected to DWT.

In Anindya Sarkar et. al.'s paper [10] the authors propose a Matrix Embedding with Repeat Accumulate (ME-RA) based steganography in which the host coefficients are minimally perturbed such that the transmitted bits fall in a coset of a linear code, with the syndrome conveying the hidden bits. The hiding blocks are pseudo-randomly chosen. A powerful repeat accumulate code is used for error correction. The authors have compared QIM (Quantization Index Modulation) and ME-RA methods. The comparisons with a slight modification of the MERA (puncture and non-shrinkage) methods with different decoding methods are also tabulated. The authors highlight that the use of ME instead of QIM within the YASS (Yet another Steganographic Scheme) that provides improved steganalysis performance but software complexity is more.

In Prosanta Gope et. al.'s article [11], the authors introduce an enhanced JPEG steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm. The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking.

In Po-Chyi et.al.'s article [12] the authors compare the advantage of embedding in JPEG 2000 images with the previous approach of embedding in JPEG images. Most of the steganographic methods are based on JPEG because as a block DCT codec JPEG lends itself a good candidate for information hiding due to its fixed block structure. JPEG 2000 which is an upcoming still image coding standard can be used to hide high

volume data. If information is embedded in the output of tier-2 coding, i.e. the JPEG 200 packets, it can be guaranteed that all the embedded information will be received without error and in correct order. But, difficulty lies in the modification of packets for embedding, since the bit-streams are compactly compressed by the arithmetic coder. Careless modification would result in failure of expanding compressed image. In the embedding process the image is decomposed using wavelet transform. (Number of wavelet decomposing levels & image size should be related to the host image), Lazy Mode Coding (Magnitude Refinement pass is suitable for steganographic purposes) is used for embedding.

In Hideki Noda et.al.'s paper [13] the authors propose a method that is based on a seamless integration of JPEG2000 lossy compression scheme and bit-plane complexity segmentation (BPCS) steganography. In bit-plane decomposition an n bit image is decomposed into a set of n binary images by bit slicing operations, combined with replacing binary data in LSB bit planes with secret data. The BPCS steganography uses bit-plane decomposition and characteristics of human vision. In JPEG 2000, wavelet coefficients of an image are quantized into a bit-plane structure. Each bit plane of the cover image is segmented into small size 8x8 blocks and are classified into informative / noise like blocks, using a threshold of the complexity $\propto_0$ (e.g. value of $\propto_{0.03}$ $\propto_{max}$). $\propto_{max}$ is the possible complexity value. The secret file is segmented into a series of blocks containing 8 bytes of data that are regarded as 8x8 binary images. If secret block is less complex than the threshold $\propto_0$, conjugate (XOR) it to make more complex. ($\propto$=$\propto_{max}$ $\propto$). The image will now be a conjugated image. Replace each noise like block in the bit planes with a block of secret data. If block is conjugated store it in the conjugation map. Blocks can be randomly selected by using a random-number generator. Also embed the conjugation map with secret data (usually the first noise like block). Secret data is embedded after tier-2 encoding.

Savita Goel et al. in [14] proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image using number of image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). Their study and experimental results shows that their proposed method is fast and highly efficient as compared to basic LSB methods.

Bingwen Feng, Wei Lu, and Wei Sun in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture" [15] purposed a state-of-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography firstly the rotation, complement and mirroring invariant texture patterns are extracted from the binary image. They also proposed a measurement and based on this proposed measurement this approach is practically implemented. Practical results show that proposed steganographic approach has high statistical security with high stego image quality and high embedding capacity.

Kazem Qazanfari and Reza Safabakhsh [16] proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from embedding of extra bits, which results in lower distortion in the co occurrence matrices. They also extend this method to preserve DCT coefficients of JPEG format images. This improved method results in fewer traces in the co-occurrence matrices then old LSB++ technique. This method is also secure against histogram based attacks because this method does not make any changes in the histogram and hence histograms of both cover image as well as stego image will be same. The quality of stego images is also high because of elimination of extra bit embedding.

On the based on Huffman Coding, Amitava Nag et al. [17] present a novel steganographic technique of LSB substitution. Their technique basically focuses on high security, larger embedding capacity and acceptable level of stego image quality. Firstly Huffman tree is produced to encode every 8 bits of secret image. After encoding, they divide the encoded bits into four parts and have 0 to 3 decimal values. Location of embedding a message in cover image is determined by these decimal values. Experimental results show that it is very difficult for attacker to extract the secret information because Huffman table decrease the size of the cover image. Purposed techniques just have acceptable level of PSNR values and lie between 30 dB to 31 dB.

P. U. Deshmuk et al. [18] also present the edge adaptive steganography based on LSB substitution. They embed secret information in sharp (edges) regions of the carrier image using adaptive scheme and difference between two adjacent pixels of carrier image. Their technique performs well than other LSB and Pixel difference based techniques and maintains the quality of stego image.

III. PROPOSED METHOD

This section describes the proposed method. First, the basic unit used in this method is called a "patch". A patch can be described as a basic block an image contains. This patch is used as a basic building block for synthetic texture. To generate synthetic texture, unique candidate patches are generated by checking for duplicate patches.

A. Preprocessing

This step includes binary to gray scale conversion of source texture image. Source texture of size 128128×128 is used. Resizing of this image into this is required.

B. Message Embedding Procedure

1) *Lookup Table Generation:* First step in message embedding procedure is lookup table generation. Lookup table is used to record the location of source patches to recover the source texture at the receiver side without any loss. This reversible style is one of the major advantage this paper offers. Let $S_w \times S_h$ be the size of the synthetic texture. Let it be488×488. Let the patch size be 48×48. Taking these values, we can generate an lookup table containing 144 entries. Then the source texture can be embedded in the synthetic texture according to the entries in the lookup table.

This offers the reversibility. Here the random seed for patch id distribution is generated based on fingerprint image of the sender. For Extraction of minutiae points from fingerprint images involves mainly 3 stages. They are preprocessing, minutiae extraction and false minutiae removal.

a) Pre-processing: This involves histogram equalization, binarization and certain morphological operations also applied to the fingerprint images. The original histogram of a fingerprint image has the bimodal type, the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced. Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0, 1 for edges and furrows respectively. After the operation, ridges and furrows are highlighted with balck and white colour. Morphological operations like hbreak, spur, thin, open, close etc. are used. Ridge thinning is used to eliminate the redundant pixels in the image. 'Open' is used to remove the peaks introduced by the background noises. 'Close' is used to eliminate small cavities.

b) Minutiae Extraction: Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. After the fingerprint ridge thinning, marking minutia points is relatively easy. For each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

c) False Minutiae Removal: This step effectively removes ridge breaks due to insufficient ink and ridge cross connections due to excess amount of ink.

d) Seed Value generation: From the minutiae point set, we can generate keys by converting it into binary and then to decimal. Finally seed generation is done by adding these keys together.

This random seed is used for generating lookup table. Initially lookup table contains -1 value in all 144 locations. We can arrange the source patches according to the id's in the lookup table. If we have 9 source patches we can arrange these patches according to the lookup table values.

2) Composition Image Generation: First, we have a blank workbench. By referring to the lookup table values we can arrange the source patches in the workbench.

3) *Texture Synthesis:* Candidate patches generated from the source texture is used to fill all blank locations in the workbench. Candidate patches are generated by shifting one pixel each in scan line order. Unique patches are generated by checking for duplicate patches.

4) *DCT Based message embedding:* Here we can embed secret message inside the candidate patches pasted in the working location. First, read the candidate patches and broke the patch into the block of 8x8.from left to right and top to bottom take the DCT of the each block .Now embed the message bit into the LSB of the DCT Coefficient. Now write the stego image by taking the IDCT of the coefficient

C. Message Extraction and Source Texture Recovery

At the receiver side, index table can be retrieved using the key shared between sender and the receiver. Using this index table source texture can be recovered by finding out positions of source patches in the stego synthetic texture. Using this source patches, source texture can be constructed without any quality loss. Secret message can also be recovered by applying DCT on the stego synthetic texture.

IV. Conclusion and Future works

This paper proposes a steganographic technique using texture synthesis. Using a source texture, this technique synthesis a synthetic texture and using fingerprint based keys, it hides the source texture. DCT based embedding technique is used to hide the secret message inside the synthetic texture so that embedding capacity is much more increased compared to the other steganographic technique. The fingerprint is unique and permanent over the person's lifetime, so fingerprint based key is more robust and is difficult to guess by the attacker. Source texture can be recovered at the receiver side without any quality loss, so that it can be used for a second round of steganography. This method is robust and it offers a large embedding capacity.

One possible future work is to combine other steganographic methods to increase the security.

References

[1] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol9, No:3, pp.405-424.

[2] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain" , International Journal of Engineering Research and Applications Vol2, Issue 3, pp. 2632-2637.

[3] Shweta Singhal, Dr.Sachin Kumar and Manish Gupta, (2011) "A New Steganography Technique Based on Amendment in Blue Factor" , International Journal of Electronics Communication and Computer Engineering, Vol.2, Issue 1, pp.52-56.

[4] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "A Generalization of the PVD Steganographic Method", International Journal of Computer Science and Information Security, Vol.8.No.8, pp156- 159

[5] Chin Chen Chang, Piyu Tsai & Min-Hui Lin (2004) "An Adaptive Steganography for Index-Based Images using

Codeword Grouping", Springer-Verlag Berlin Heidelberg 2004, pp.731- 738.

[6] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) "Comparison of Secure and High CapacityColor Image Steganography Techniques in RGB and YCBCR domains" , International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[7] Hemalatha.S, U.Dinesh Acharya and Renuka.A, Priya.R Kamnath, (2013) "A Secure and High Capacity Image Steganography Technique", Signal & Image Processing , An International Journal, Vol.4, No.1, pp.83-89.

[8] Keith L.Haynes, (2011) "Using Image Steganography to Establish Covert Communication Channels", International Journal of Computer Science and Information Security, Vol 9, No.9, pp. 1-7.

[9] S.Arivazhagan, W.Sylvia Lilly Jebarani, and S.Bagavath (2011) "Colour Image Steganography Using Median Maintenance" , ICTACT Journal on Image and Video Processing, Vol. 2, Iss:01, pp.246-253.

[10] Anindya Sarkar, Member, IEEE, Upamanyu Madhow, Fellow,IEEE, and B.S.Manjunath, Fellow, IEEE, (2010) "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography" , IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.225-239.

[11] Prosanta Gope, Anil Kumar and Gaurav Luthra , (2010) "An Enhanced JPEG Steganography Schemewith Encryption Technique" , International Journal of Computer and Electrical Engineering ,Vol.2.No.5, pp924-930.

[12] Po-Chyi & C.-C.Jay Kuo, Fellow, IEEE(2003) "Steganography in JPEG 2000 Compressed Images", IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp 824-832.

[13] Hideki Noda, Jeremiah Spaulding, Mahdad.NShirazi & Eiji Kawaguchi (2002) "Application of Bit-Plane Decomposition Steganography to JPEG 2000 Encoded Images" .

[14] S. Goel, S. Gupta, and N. Kaushik, "Image Steganography Least Significant Bit with Multiple Progressions" , Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), vol. 2, Springer (2014).

[15] B. Feng, W. Lu, and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE transactions on Information Forensics and Security, vol. 10, no. 2, (2015).

[16] K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier International Journal of Information Sciences, vol. 277, (2014).

[17] A. Nag, J.P. Singh, S. Biswas, D. Sarkar, and P. P. Sarkar, "A Huffman Code Based Image Steganography Technique" , 1st International Conference on Applied Algorithm (ICAA), (2014) January 13-15, Kolkata, India.

[18] P. U. Deshmukh and T. M. Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique", IEEE International Conference on Information Communication and Embedded Systems (ICICES), (2014) February 27-28, Chennai, India.