International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.8, No.7 (2015), pp.161-170
http://dx.doi.org/10.14257/ijsip.2015.8.7.15

State-of-the-art Review on Steganographic Techniques

Satwinder Singh[1] and Varinder Kaur Attri[2]

[1, 2] Computer Science & Engineering Department
GNDU RC, Jalandhar, India
[1]er.satwindermehmi@gmail.com,[2]varinder2002@yahoo.com

Abstract

Information security is one of most important concern in any communication. There are number of security attacks related to information security and number of techniques has been implemented to prevent these attacks. Data hiding is related field to information security. Data hiding can be achieved be using Digital Steganography. Digital Steganography is art of hiding secret messages behind the innocent looking digital media. In this paper we have done state-of-the-art survey on image steganographic techniques and steganographic techniques used with different cryptographic algorithms, to provide extra layer of Security.

Keywords: *Steganography, Cryptography, Digital Image, Security, Encryption*

1. Introduction

In ideal situation we expect language to be something which is easily understandable, shared and reliable. However, in real life the dialects, different kinds of foreign languages, security or communication system prevent this ideal situation and sometimes make understanding out of our reach. Sometimes the concept of "What You See Is What you Get (WYSIWYG)" may not hold true in all the situations. Which means what you see is not necessarily what you get. Innocent looking images or any other media content can be more than what be seen with the Human Visual System. They can convey more than what they can.

The word "Steganography" is a Greek word which literally means "covered or hidden writing". In other words Steganography is an art and science of hiding secret information behind the cover medium. It is the art of concealed communication. Cover medium can be any multimedia content like digital images, audio files or video files. The main motive of steganography is to hide the existence of communication [1]. To understand the concept of steganography let us consider an example of two friends want to communicate in secret manner. Alice wants to send some secret information to his friend Bob. Alice starts by writing a letter to his friend describing his recent summer camp experiences. After he finished writing, Alice replaces the ink with the milk and writes down the secret message in between the inked lines of his letter. After sometime when milk dries, the secret message becomes invisible to human visual system. To see the hidden secret message bob try to heat the paper above the candle. This heating process reveals the hidden secret message. This is an example of steganography.

Steganography, watermarking and cryptography are the three fields which are closely related to each other and belong to same family i.e. Security. Steganography and watermarking process is very difficult to tease apart especially for those which are from different disciplines. Figure 1 demonstrates the taxonomy of security system where bold face text represents the focus of this study.

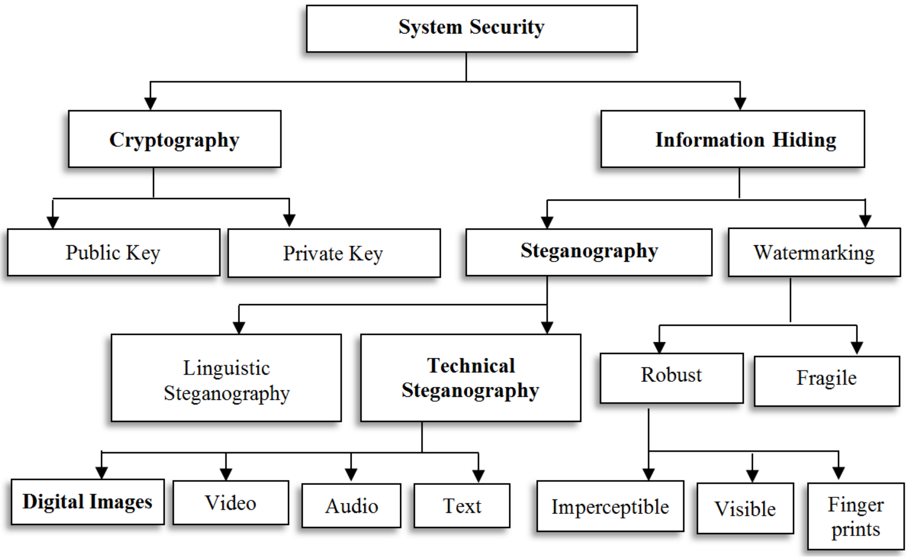

Figure 1. Taxonomy of Security System [2]

Security systems consist of three components namely, Cryptography, Steganography and Watermarking. Last two techniques come under information hiding.

1.1. Steganography vs. Cryptography

Steganography and cryptography are cousins which belong to same family of data security. Cryptography is an art of converting plain data to the unreadable form. It is a process of scrambling the plain text into cipher text using some cryptographic algorithms. Cipher text can't be understandable by anyone. On the other hand, as mentioned, Steganography is process of hiding data behind the cover medium using steganography algorithms. Both steganography and cryptography can be utilized to provide extra layer to the security framework.

1.2. Steganography vs. Watermarking

There is very important difference between steganography and watermarking. In steganography secret information must never be visible to viewer unaware of its presence. On the other hand this feature is optional in watermarking process. Watermark may or may not be visible to its viewer depending on the requirement of the application.

2. Types of Steganographic Techniques

2.1. Spatial Domain Steganography

In spatial domain steganographic techniques secret information is directly embedded in pixel values i.e. pixels are directly altered to store secret messages. Basically these techniques are very simple but have greater impact then other techniques.

2.1.1. Least Significant Bit Substitution Algorithm: LSB substitution algorithm is simplest form of algorithm in which LSBs of the cover image is modified according to the secret message. It is simple yet effective technique of embedding secret data into images. Each pixel is of 8 bits in case of Gray scale images. Color RGB images use 24 bits to store color information each 8 bits for Red, Green and Blue components.The Advantages of this algorithm is simplicity and high perceptual efficiency. It can also achieve high embedding capacity but this algorithm is sensitive to image manipulations such as cropping, scaling and rotations, Lossy compression and addition of noise. There are number of variations of this algorithm including Edge and texture masking of cover image to determine the number k bits of LSBs for data embedding [3], Adaptive LSB algorithm based on brightness, optimized LSB algorithm using cat swarm and genetic algorithm [4,5], image steganography based on histogram modifications [6,7] etc. This research work mainly focuses on LSB steganography algorithm, so the rest of all the algorithms available in the literature will not be discussed in detail.

2.1.2. Pixel Value Differencing: This technique sub divides the cover image into non overlapping blocks consisting of two connecting pixels. This technique hides the data by altering the difference between two connected pixels. High difference in the cover image pixel value allows the higher alterations. Area of the pixel decides the hiding capacity of this technique for example if edge area is chosen then the difference is high in between the connecting pixels. Whereas in smooth areas, difference is low. So ideal choice is to select edge areas to embed the secret message that is having more embedding capacity. Stego image produced by this technique has more quality and has better imperceptibility results [8].

2.1.3. Grey Level Modification: In this technique data is mapped by applying some modifications to the gray values of the image pixels. This technique will not hide or embed data, instead it map the data by using some mathematical functions. Set of pixels are selected for mapping using this mathematical function. It uses the concept of odd and even numbers for mapping the data in cover image. High hiding capacity and low computational are some advantages of this technique [9].

2.1.4. Prediction based Steganography: In this technique pixel values are predicted with the help of predicator. This technique removes the loopholes of other techniques which directly embed the secret data into pixel values. In order to improve hiding capacity and visual quality it uses prediction error values (EV). EVs are altered to hide the secret data. It consists of two steps, namely prediction step and entropy coding. In prediction step predicators are used to determine the pixel values of a cover image and in the second step entropy coding of prediction error values is done.

2.1.5. Quantization Index Modulation (QIM): Quantization index modulation is technique of spatial domain steganography in which secret information is embedded in cover image by modulating an index with embedded information and after that quantization process is applied to the host signal with associated quantizer(s). This technique has number of advantages such as high embedding capacity and is highly robust technique.

2.2. Transform or Frequency Domain Steganography

Transform domain steganography techniques are the most complex way to embed the secret data in the cover image. Any image in digital form is made up of high and low frequency components. Digital image can have smooth and edge (sharp) areas. Smooth areas represent low frequency whereas high frequency is represented by edge or sharp areas of the cover image. Changes done in low frequency areas can easily be visible to human eyes. So it is not possible to embed equal amount of secret information in all the regions. It has number advantages over the spatial domain methods of steganography such as it is more robust against compression, image processing and cropping and these methods are less prone to attacks. These techniques are not dependent upon image file format. Transform domain steganography techniques are broadly classified into following types:

2.2.1. Discrete Wavelet Transformation Technique: Discrete wavelet transformation techniques divides the cover image into four sub bands where higher band represent finer details and lower band has more important information. Entropy coders locate the transform coefficients and encode them. DWT technique has extra edge over DCT that it offers efficient energy compaction than DCT without any blocking artifacts after the process of coding. DWT has multi-resolution nature that make it best fit for scalable image coding. There are several other types of transforms that can applied with DWT such as integer transform, curvelet transform, contourlet transform, dual tree DWT etc.

2.2.2. Discrete Cosine Transformation Technique: Discrete cosine transformation is very famous steganography techniques which is best suited for JPEG images. JPEG images are widely used over the internet and have lossy nature of compression. DCT is extensively used for image and video compression. Every block of DCT is quantized with the help of quantization table of JPEG. Quantized coefficients are used to embed the secret message. Afterward coding methods are applied such as Huffman coding. In this technique high frequency regions are better for information hiding as they often become zero after the process of quantization. Hence it is not necessary to modify the coefficient value if the embedded data is zero. JSteg/ JPHide, F5, YASS (Yet another steganographic scheme) and Outguess are some of the DCT steganography tools.

2.3 Spread Spectrum Steganography

Spread spectrum is very famous technique in digital and wireless communication. It is process in which bandwidth of narrow band is modulated across the wider band of frequencies. After spreading, resulting signal is added with the cover image and the output image is stego image with secret information in it. Embedded signal has very low power which is very difficult to detect the presence of steganography. So in this case Signal-to-Noise (SNR) is very less. It must require synchronizing of pseudo random noise generated at transmitter as well as receiver end to generate desired results [10]. This technique uses symmetric key system that requires transmitter and receiver to use same key for communication. Advantages of this technique are good stego image quality and it maintains the robustness against various attacks. It is very difficult for the attacker to detect and extract the embedded secret information. There can be further improvements that can enhance the embedding capacity and reduce the bit error rate during embedding process. Peak-signal-to-noise-ratio (PSNR) and Mean square error (MSE) can be used to analyze the performance of this steganographic algorithm in term of stego image quality with respect to original cover image.

2.4. Adaptive Steganography

Number of advantages of transform domain steganographic methods over image or spatial domain technique encourages the use of these techniques. Adaptive steganography is also known as model based steganography or Statistics-aware embedding. In this technique statistical properties of the cover image is used. This technique embeds the secret information in cover image without changing its properties. It can be of two types, in first we select random adaptive pixels depending on cover image and in the second we select those pixels which have higher local standard deviation value. This technique has large embedding capacity and it provide high security to the stego image against various attacks. So every steganographic method has its own merits and demerits. Depending upon the type and requirement of application one can use a method which is best fit his/her requirements.

3. Literature Review

3.1. State-of-the-Art Review on Steganography Techniques

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

G. Prashanti and K. Sandhyarani [11] have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

Savita Goel *et al.* in [12] 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.

Della Baby *et al.* [13] proposed a “Novel DWT based Image Securing method using Steganography”. In their work new steganography technique is prosed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors *i.e.* Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using this system has good robustness. Value of PSNR and SSIM index have been used by authors to compare the quality of stego image and original cover image. Proposed method has good level of PSNR and SSIM index values. Authors have found that their experimental results are better than existing approaches and have increased embedding capacity because of data compression. So security is high with less perceptible changes in stego image.

Bingwen Feng, Wei Lu, and Wei Sun in their paper “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture” [14] 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.

M. Nusrati *et al.* [15] have done study on heuristic genetic algorithm based steganographic method for hiding secret information in a cover image. This method optimally find the appropriate locations in cover image to embed the secret information by focusing on the “before embedding hiding techniques”. It tries to make least changes in the bits which lead to minimal modifications in image histogram. To covert the LSBs and secret message to set of blocks, segmentation is done in this genetic algorithm. After this algorithm finds the appropriate locations for embedding, the secret blocks are embedded and it generates the key file which is used during message extraction process.

Experimental results show that this genetic based method is more efficient than basic LSB algorithm with high stego image quality.

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.

N. Akhtar et al. in [18] present and implement the improved version of traditional LSB image steganography technique. Their work enhances the quality of stego image using bit inversion method. They propose and implement two approaches of bit inversion techniques. These both techniques resolves around bit inversion techniques in which LSBs of pixels of carrier image are inverted only and only if they arise with specific pattern of pixel’s bits. This leads to lesser modification in pixels is compared to traditional LSB method. For correct retrieval of secret message, inverted bits need to be embedded somewhere within the stego image. Experimental results demonstrate that PSNR value of stego image is improved; hence stego image quality is improved.

P. U. Deshmuk et al. [19] 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.

E. Dagar and S. Dagar [20] present the steganography technique for color RGB images to improve the security level of data transfer through the internet. 24 bit RGB image is utilized as cover image to embed secret data in red, green and blue pixels. X-Box mapping is used and several boxes contain 16 different values. Here “X” represent any integer number from 0 to 9. After this values saved in X-Boxes are mapped with LSBs of carrier image. It is very difficult for the attacker to extract the secret information because they make use of mapping. Thus this mapping provides high level of security to hidden information. PSNR value is also calculated and it has high PSNR value which leads to greater stego image quality.

M. R. Modi et al. [21] proposed a novel steganography technique to embed secret information of LSBs of cover image. In their method least two significant bits of edges are utilized to store secret message as edge regions are very good areas to embed the secret information than other smooth regions of cover image. In this method edge region are detected on basis of amount of secret information, which means it does adaptive edge detection. Experimental results analysis shows that their method performs better than traditional LSB image steganographic methods and has greater security against visual attacks.

D. Samidha and D. Agrawal [22] in their research paper “Random Image Steganography in Spatial Domain” study various image steganographic methods and proposed a LSB based steganography method using random bit selection. In their techniques least significant bit is selected randomly for embedding the secret information inside the cover image. They also proposed some more techniques based on random pixels of cover image and secret information is embedded in randomly selected bits of random pixels. Intensity values, location of pixels etc. parameters are used for this purpose.

Che-Wei Lee and Wen-Hsiang Tsai in [23] proposed a new method of steganography which uses PNG images to hide secret information. Shamir's method for secret sharing is utilized to produce partial shares from the given data string with the help of some polynomial's coefficients as data carrier for computing the shares. These partial shares are then embedded into Alpha channel (Transparent regions) and generate the stego image which has white noise. Small prime number can be used to reduce the white noise. Proposed method has effective data capacity of hiding data with enhanced security level and stego image quality.

3.2. Review on Encryption Technique Used with Steganography

This section covers some of the studies that utilize both steganographic and cryptographic techniques in order to gain extra layer of security to the hidden data.

D. Debnath *et al.* [24] proposed a security scheme in which steganography is used along with cryptography to provide better security to embedded data. In their method first data is encrypted then it is embedded into cover image using steganographic method. Proposed algorithm transforms any kind of message into text with the help of manipulation tables, and then carries out hill cipher methods to it and finally hides the data into red, blue, and green pixels of the cover image. They use number of image quality parameters like MSE, PSNR, AD, SC, NAE and MD.

D. E. M. Ahmed and O.O. Khalifa in [25] present a technique in which LSB image steganography is used along with Elliptic Curve Cryptography (ECC) to offer greater security to data. In the proposed work sender is allowed to choose a suitable cover image and secret information. In this process secret information is first encrypted using elliptic curve cryptography and then this ciphered secret information is embedded into cover image using least significant bit image steganography method.

M. R. Islam *et al.* [26] proposed a new improved version of LSB image steganography based on efficient filtering technique using status bit. Proposed work also use AES algorithm for encryption proving extra layer of security. In their work bitmap images are used because of their uncompressed nature and bitmap images are best suited for LSB based steganography. In this method first secret data is encrypted using AES algorithm and then this encrypted data is embedded into image using steganographic process. Improved steganographic method is proposed which can embed more secret information using filtering based algorithm and for the filtering purpose MSB of bitmap image is utilized. Proposed work also makes use of status bit for checking insertion and extraction of secret messages. Experimental results demonstrate that this method has high embedding capacity than basic LSB algorithm. PSNR values are also high because of high stego image quality. All the experimental results prove that this method is more efficient than traditional LSB method for hiding the data in bitmap images.

S. Krishnagopal *et al.* [27] proposed a system as whole which contains the features of both steganography and cryptography. They make use of Chaos based cryptographic methods to develop encryption algorithm. Chaotic logistic and cat map are used as a base for their image encryption algorithm. In their method of image encryption the secret key is altered after encrypting every pixel of the image with the application of Arnold's Cat map. This concept of altering secret key after encryption makes this system more robust against various attacks. In the next phase, encrypted image is embedded into cover image using image steganography. Simulation results are carried out on the basis of some parameter like SSIM index and PSNR. Results show that their system has 0.981 SSIM index value and 47.71 dB PSNR. So it generates very good quality of stego image and it is more efficient and secure against attacks and can be used for real time image encryption and transmission.

S. Song [28] *et al.* proposed a very innovative system that will combine the steganography and cryptography into one system. There will be no separate computations for steganography and cryptography. Hence this system needs lesser computations than existing methods, while maintain the higher security levels. Core of this system is LSB matching technique and Boolean function in stream ciphers. For steganography gray scale images are utilized and Boolean functions are applied for cryptographic purpose and to control the pseudo-random increment and decrement of LSBs. Experimental results shows that this system is very much safer from steganalysis attacks.

4. Conclusions

The word Steganography is derived from Greek origin which means “Cover Writing”. Steganography have been used from ages and set its roots from ancient Greece. Null Ciphers, Microdots and invisible ink methods were also very popular steganographic methods during ancient times. All these techniques encourage the modern day engineers and scientists to invent some more steganographic methods in digital era of computers. This paper reviews the basic steganographic techniques and state-of-the-art review on these modern day steganographic techniques. Performance of each technique is also discussed in Literature Review section and main focus of our study is on image based steganographic methods. It is observed that the embedding procedure is easy in spatial domain steganographic techniques and compare to complex transform domain steganographic techniques. Spatial domain techniques are simple and have high stego visual quality, whereas transform domain techniques are more robust and less prone to image processing attacks. So this paper reviews different types of embedding secret messages with their advantages and disadvantages.

References

[1] K.B. Raja, C.R. Chowdary, K.R. Venugopal and L. M. Patnaik, “A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images”, Proceeding of 3rd IEEE International conference on Intelligent Sensing and Information Processing (ICISIP), **(2005)** December 14-17, Bangalore, India.

[2] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, “Digital image steganography: survey and analysis of current methods”, Signal Processing, vol. 90, no. 3, **(2010)**.

[3] H. Yang, X. Sun, and G. Sun, “A High-Capacity Image Data Hiding Scheme using Adaptive LSB Substitution” , Radio Engineering, vol. 18, no. 4, **(2009)**.

[4] Z. H. Wang, C. C. Chang, and M. C. Li, “Optimizing Least Significant Bit Substitution using Cat Swarm Optimization Strategy”, Information Sciences, vol. 192, no. 1, **(2012)**.

[5] S. Wang, B. Yang, and X. Niu, “A secure steganography method based on genetic algorithm”, Journal of Information Hiding and Multimedia Signal Processing”, vol. 1, no. 1 **(2010)**.

[6] Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, “Reversible Data Hiding Based on Multilevel Histogram Modification and Sequential Recovery”, International Journal of Electronics and Communication, vol. 65, no. 10, **(2011)**.

[7] C. C. Lin, W. L. Tai, and C. C. Chang, “Multilevel Reversible Data Hiding Based on Histogram Modification of Difference Images”, Pattern Recognition, vol. 41, no. 12, **(2008)**.

[8] D. Wu, and W.H. Tsai, “A Steganographic Method for Images by Pixel Value Differencing”, Pattern Recognition, vol. 24, no. 9-10, **(2003)**.

[9] V. M. Potdar, and E. Chang, “Gray Level Modification Steganography for Secret Communication”, Proceeding of 2nd IEEE International Conference on Industrial Informatics (INDIN), **(2004)** June 26-26, Berlin, Germany.

[10] L. M. Marvel, C. G. Boncelet, and C. T. Retter, “Spread Spectrum Image Steganography”, IEEE Transaction on Image Processing, vol. 8, no. 8, **(1999)**.

[11] G. Prashanti, and K. Sandhyarani, “A New Approach for Data Hiding with LSB Steganography”, Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, vol. 2, Springer **(2015)**.

[12] 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)**.

[13] D. Baby, J. Thomas, G. Augustine, E. George, and N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, vol. 46, **(2015)**.

[14] 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)**.

[15] M. Nusrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm", 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), **(2015)** February 21-22, Haryana, India.

[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] N. Akhtar, S. Khan and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), **(2014)** February 7-8, Ghaziabad, India.

[19] 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.

[20] E. Dagar and S. Dagar, "LSB based Image Steganography using X-Box Mapping", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), **(2014)**, September 24-27, New Delhi, India.

[21] M. R. Modi, S. Islam and P. Gupta, "Edge Based Steganography on Colored Images", 9th International Conference on Intelligent Computing (ICIC), **(2013)** July 28-31, Nanning, China.

[22] D. Samidha and D. Aggrawal, "Random Image Steganography in Spatial Domain" IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), **(2013)** January 7-9, Tiruvannamalai, India.

[23] C. Lee and W. Tsai, "A New Steganographic Method Based on Information Sharing via PNG Images", IEEE 2nd International Conference on Computer and Automation Engineering (ICCAE), **(2010)** February 26-28, Singapore.

[24] D. Debnath, S. Deb, N. Kar, "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography", IEEE International Conference on Computational Intelligence and Networks (CINE), **(2015)** January 12-13, Bhubaneshwar, India.

[25] D.E.M Ahmed and O. O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography", IEEE International Conference on Computer and Communication Engineering (ICCCE), **(2014)** September 23-25, Kuala Lumpur, Malaysia.

[26] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE International Conference on Informatics, Electronics & Vision (ICIEV), **(2014)** May 23-24, Dhaka, Bangladesh.

[27] S. Krishnagopal, S. Pratap and B. Prakash, "Image Encryption and Steganography Using Chaotic Maps with a Double Key Protection", 4th International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing, **(2014)** December 24, India.

[28] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advanced in Control Engineering and Information Science, vol. 15, **(2011)**.

Authors

Satwinder Singh, He received the graduate degree of bachelor of technology in computer science and engineering from Punjab Technical University, Jalandhar, India in 2013 and post graduate degree of Master of Technology in computer science and engineering from Guru Nanak Dev University, Amritsar, India in 2015. His research interest includes Digital image steganography, Information security and Encryption.

Varinder Kaur Attri, She received the graduate degree of bachelor of technology in computer science and engineering from Punjab Technical University, Jalandhar, India in 2000 and post graduate degree of Master of Technology in computer science and engineering from Punjab Technical University, Jalandhar, India in 2009. She is pursuing Ph.D. from Punjab Technical University and working as an Assistant Professor at Guru Nanak Dev University, Regional Campus Jalandhar, India. Her research interest includes Software Engineering.