International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.259-282
http://dx.doi.org/10.14257/ijsia.2016.10.3.24

Critical Analysis of Steganography "An Art of Hidden Writing"

Aqsa Rashid[1], Muhammad Khurrum Rahim[2]

Department of CS&IT, Islamia University of Bahawalpur, Pakistan[1],
Department of EE, NUCES, FAST, Pakistan[2]
aqsarashid2@gmail.com[1], aqsa.rashid.pk@ieee.org[1] khurrumrahim@gmail.com [2]

Abstract

Steganography is the art of hiding information inside another medium while the presence of this embedding is invisible by human perception. In disparity to cryptography, steganography have a tendency to conceal the presence of the message or communication appearance, while cryptography tries to hide the content of the clandestine message. Hiding the presence of message or communication can be made by inserting a clandestine message into the clear cover medium which no one besides the correspondent and the receiver can imagine. This paper present the review and critical analysis of steganography methods projected during the recent years that are from 2011 to 2015. Many schemes are mentioned with their technical terms, main logic, advantages and disadvantages in terms of important measures. Critical analysis is based on the type of cover object used, domain of the algorithm and important properties that are used as evaluative measures for steganographic system.

Keywords*: Steganography; hidden writing; cover object; stego object; embedding; extraction*

1. Introduction

Steganography is a gifted approach in the current era of digital technology. Due to its effectiveness it is gaining importance rapidly. Steganography has established a lot of consideration in few years [1, 2, 3, 4, 5, 6, 7, and 8]. In view of the fact of September 11th, 2001, some people have recommended that Al Qaeda employ Steganography method to synchronize the World Trade Centre attack. But later, nothing was provided as evidence. Some scientific and commercial application of the hidden writing includes that it is the most important tool for the secure electronic transmission of important information, document authentication, document tracking, digital election and electronic money. Beside these, information collected in a radar station, or during medical imaging, can be put together with the pictures.

The survey includes various papers on hidden writing methodology from 2011 to 2015. Most achievable schemes presented in this time period are tried to include in this review.

1.1 Steganography System

A complete steganography system consists of the cover object, stego object, embedding algorithm, extraction process and secret message and some time a stego key which is used to extract the message from stego object. Explanations of the important terminologies of the stego system are following:

ISSN: 1738-9976 IJSIA

- **Cover Object:** It is the input image, video file, audio file or a text file in which concealment of secret data is to be performed.
- **Stego-Object:** After the concealment of secret data into the cover medium, the cover object becomes the stego-object.
- **Embedding:** Embedding is the process of making a stego-object from a cover object. Or we can define it as the process of concealment of secret message into some digital medium.
- **Extraction:** This is the reverse process of embedding. In this process, the conceded message is recovered from stego-object to read it.
- **Message:** It is the secret information that is to be embedded in the cover object for safe transmission of data from sender to receiver.

1.2 Cover Medium Used for Steganography

Different digital medium are used as cover medium for hiding the data. On the basis of medium, steganography is named accordingly. These include the following:

- **Image Steganography**: Steganography that uses image as cover medium is named as Image steganography. Secret data is embedded or concealed in the pixel data of the image.
- **Video Steganography:** In video steganography, secret data is concealed in video file format. A video file is defined as series or combination of images. Mp4, AVI, MPEG and other video format are used as cover object in video steganography.
- **Audio Steganography:** Audio file act as a cover medium in audio steganograogy. This medium has turn into very considerable medium due to VOIP (voice over IP) reputation.
- **Text Steganography:** In text steganography, white spaces, tabs, capital letters etc are used to complete the process of steganography.

1.3 Classification Based on Domain of Steganography

On the basis of processing, it has been classified in the following different domains:

- **Spatial Domain Scheme:** These methods have many versions. All of these directly create a change or process some bits of the pixel or directly process the pixel for concealing the secret data. Some very common spatial domain methods are based on LSB (Least significant bit) Based, PVD (Pixel value differencing) Based, Texture Based, Pixel Intensity Based, Histogram Shifting Based, Connectivity or Labeling Based, Pixel Mapping Schemes, Edge Based Embedding Schemes etc. Mostly the spatial domain methods are effective, good, medium complexity, create less degradation in medium and hide more data. But they are less robust and could be destroyed by attacks.
- **Transform Domain Scheme:** Transform domain method have the plus point over the spatial domain method that these schemes conceal the secret data in the specific region of the medium that is more robust. But the complexity of these schemes is more complex than the spatial domain methods. DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), Lossless or reversible, concealing in coefficient bits etc are transform domain methods.
- **Hybrid Scheme:** In hybrid approaches some part of the processing is performed in spatial domain and some is in transform domain. Although the security level increases but the complexity reaches at its maximum level.

Table 1 shows the comparison of the spatial, transform and hybrid schemes of the steganography.

Table 1. Comparison of Spatial, Transform and Hybrid Domain Methods

Property	Spatial	Transform	Hybrid
Complexity	Less	More	Most
Robustness	Less	More	More
Capacity	Increased	Medium	Medium
Actual Logic	Directly processing with bits.	Find Robust region for concealing.	Some Part in Spatial domain and embedding in transform domain

1.4 Important Steganographic Measures

Some important properties which act as steganographic measures of a good stego-system include the following:

- **Visual Quality:** It is the perceptual appearance of the image. For a good stego method, visual quality should be undistinguishable from the cover image.
- **Complexity**: How much it is expensive and time consuming to embed and extract the message. For good stego scheme, complexity should be least.
- **Capacity:** Total number of bits that could be hidden in the cover file is called the capacity of that file. Stego system should have high embedding capacity.
- **Robustness:** It depends on the property that after any transformation data should stay intact.
- **Invisibility:** Statistical change should be as low as possible or have least change so that difference between cover file and stego file is very difficult to detect.
- **Temper confrontation:** How much it is difficult to change the message once it has been embedded in some cover medium.

For the current analysis the

1. Visual Quality property will be measured as: E=Excellent, G=Good, P=Poor
2. Complexity property will be measured as: H=High, M=Medium, L=Low
3. Capacity will be measure as: I=Increased, M=Medium
4. Robustness will be measured as: M=More robust, L=Less robust
5. Invisibility will be measured as: Y=Yes, N=No
6. Temper confrontation will be measure as: H=High, M=Medium, L=Low

For steganography, if the visual quality is excellent or good, complexity is low, system has increased or medium capacity, highly more robust, invisible and temper resistance then the steganography approach is considered as effective and good approach. Table 2 shows the evaluation criteria for the steganographic schemes.

Table 2. Evaluation of Steganography Technique

Measure	Advantage	Disadvantage
Visual quality	E,G	P
Complexity	L	M, H
Capacity	I,M	
Robustness	M	L
Invisibility	Y	N
Temper confrontation	H, M	L

2. Critical Analysis of Steganographic Techniques

Table 3 shows the comprehensive literature survey of 100 papers in which all the papers are arranged in descending order of their publication year. Different methods were

used by different authors in different years are pointed out clearly along with their plus point and disadvantages.

Table 3. Literature Reviewed

Author	Year	Cover Medium	Domain	Technical Terms	Important Characteristics	Advantages/ Disadvantages					
		Image/ Video/ Audio/ Text/ network	Spatial/ transform/Hybrid/ Other			Visual Quality	Complexity	Capacity	Robustness	Invisibility	Temper confrontation
Aqsa Rashid [9]	2015	Image	Spatial	Mod function, Electronic Communication, Robust, LSB, GLM, Matching, Substitution	Define a mod function. Use three bits next to the least significant bit. If the binary of mod value and the message bits are equivalent then no adjustment needed. Otherwise process of adjustment need to be performed.	E	M	M	H	Y	H
Debnath, D. ; et al. [10]	2015	Image	Spatial	MSE, PSNR, SC, AD, MD, NAE, Hill Cipher, Histogram	Projected method is a crypto-stego model. Encryption is performed by hill cipher method. Encrypted message is then embedded in the image.	E	H	M	M	Y	H
Nosrati, Masoud; et al. [11]	2015	Image	Spatial	Genetic algorithm, Segmentation, LSB	Find proper location or place in the cover image for embedding. After embedding it creates a key file for the extraction process.	E	H	M	M	Y	H
Feng, B., et al. [12]	2015	Image	Spatial	HVS, Texture, Complement, LTP, mirroring-invariant, rotation	Extraction of LTP is required. Diminish the inserting alteration. Manage statistical protection without affecting the image visual quality or the inserting capacity.	E	M	M	M	Y	M
Wu, K. , et al…[13]	2015	Image	Spatial	TS, stego- synthetic texture	Reversible texture synthesis concept is used Embedding process does not affect the image quality.	E	M	M	M	Y	M
Pan, Z. , et al…[14]	2015	Image	Spatial	VQ, biased-distribution	Reversible data concealing scheme for VQ indices Improved presentation in inserting capacity, the inserting effectiveness and bit rate.	E	M	H	M	Y	M

M.Khurrum.R, et al…[15]	2014	Image	Spatial	LSB, Substitution, Matching, MSE, PSNR, UIQI, SSIM,	Matching on second least significant bit Substitution on least significant bit Histogram analysis gives good result IQMs have least changes	E	M	H	M	Y	L
Khupse, S. , er al…[16]	2014	Video	Spatial	ROI, RGB, YcbCr	Detect skin region and use it as the region of interest to hide data Embedding require conversion of RGB to YCbCr color space. After embedding YCbCr to RGB conversion required	E	H	H	M	Y	M
Akhtar, N. , et al… [17]	2014	Image	Spatial	Lossless, MBS , restoration	(MBS) Module-based substitution scheme can hide either text, image or wav file as secret data Retrieval process is lossless	E	M	M	M	Y	H
Banerjee, I.; et al… [18]	2014	Image	Transform	Frequency Domain, DCT, PFM	Use the prime factor mapping Robust method depend on pixel factor mapping	E	H	M	M	Y	H
Goswami, S.; et al…[19]	2014	Image	Spatial	JPEG, LSB	No Pre-processing is required undetectable distortion with increased hiding capacity Security of data depend on length of key	E	L	H	M	Y	H
Gupta, N.; et al… [20]	2014	Audio	Hybrid	DWT, LSB	Discrete wavelet transformed based and least significant based Better than simple least significant bit.	E	H	M	M	Y	H
Darabkh, K.A.; et al…[21]	2014	Image	Spatial	3D Geometric shapes, LSB, Substitution, Replacement, PSNR	dispense the clandestine message in one share of the image Reform of shape is difficult process for hackers	E	L	M	M	Y	M
Senthooran , V.; et al… [22]	2014	Image	Transform	DCT, LSB, Quantization Table, MSE, PSNR	Permit large data insertion capacity without image squalor.	E	H	H	M	Y	H
Shripriyadharshini, T.S.K.; et al… [23]	2014	Image	Spatial	Reversible Data Hiding (RDH),	Cover image can be restored i.e., lossless method Two keys used in decryption process Better image quality	E	H	M	M	Y	M
Chou, Yung Chen; et al… [24]	2014	Image	Spatial	inverse S-scan order, pixel segmentation, and histogram shifting	enhance the data embedding capacity Use inverse S-scan order, segmentation and histogram shifting in processing	E	H	H	M	Y	M
Al-Dmour, H. ; et al… [25]	2014	Image	Spatial	Pixel Value Differencing (PVD), region of interest (ROI), Region of Non-Interest (RONI).	Pixel Value Differencing (PVD) recognizes contrast area in the image. Hamming code that embeds secret message bits. To protect the content of the ROI, the embedding is only performed using the RONI	E	H	H	M	Y	M

Sarreshtedari, S. ; et al… [26]	2014	Image	Spatial	LSB matching, Histogram	A better imperceptibility and also higher robustness against well-known LSB detectors. reduces the probability of change per pixel to one-third without sacrificing the embedding capacity	E	L	M	M	Y	M
Roy, Ratnakirti ; et al…[27]	2014	Image	Spatial	Entropy, ROI	Use image entropy for segmentation Segmentation is performed to segment smooth and textures are Variable data rate insertion is performed	E	L	M	M	Y	M
Chi-Yuan Lin ; et al… [28]	2014	Image	Spatial	matrix embedding (ME),	Use convolution to increase the embed capacity For embedding, the time-varying convolution code is used.	E	L	M	M	Y	M
Huynh Ba Dieu ; et al… [29]	2014	Audio	Transform	Amplitude	Modifies the amplitude of cover audio file Key is used to hide the secret message Blind method of steganography	E	H	H	M	Y	H
Gutierrez-Cardenas, J.M.[30]	2014	Image	Spatial	PRNG, Secret Key	Secret key steganography Perform mapping with PRN and key Leave the cover and stego image unchanged.	E	L	M	M	Y	M
Kedmenec, L. ; et al… [31]	2014	Image	Transform	DCT, bit error rate (BER)	BER for different hit is less than 1%. Hide data by changing the coefficients in the cosine domain	E	H	H	H	Y	H
Yajam, Habib Allah ; et al…[32]	2014	Image	Spatial	lexical substitution	Secret Key Stego scheme provides short length stego keys and significant robustness against active adversary attacks	E	M	M	L	Y	M
Bidokhti, Amir ; et al…[33]	2014	Image	Spatial	wet paper embedding	High embedding effectiveness. Offer suppleness for selecting the inserting load, particularly in lower payload circumstances	E	M	M	L	Y	M
Roy, S. ; et al… [34]	2014	Image	Spatial	CNP (Card Not Present), cryptography	Crypto-stego Model Double security level	E	M	M	L	Y	M
Kumar, S. ,et al… [35]	2014	Video	Transform	PSNR, MSE, DWT	Wavelet transformation scheme Image is watermarked on Video frame Improved result of dissimilarity measure	E	H	H	M	Y	H
Gupta, P.K. ; et al…[36]	2014	Image	Spatial	Least Significant Bit Replacement (LSBR), optimal pixel adjustment process (OPAP), Peak Signal to Noise Ratio (PSNR)	Randomly disperse that secret message bits Harder to detect the inserted secret data	E	M	M	L	Y	M

Mandal, Ashis Kumar ; et al… [37]	2014	Audio	Spatial	LSB, stereo-audio samples	important perfection of LSB technique Stego-key and its parity are used to embed the secret data bit in cover audio sample Improved imperceptibility and security	E	M	M	L	Y	M
Chou, Yung Chen ; et al…[38]	2014	Image	Spatial	PDHS, Ripple scheme,	Reversible message hiding method Depend on PDHS (pixel difference histogram shifting) and ripple policy. Ripple technique is used to compute the difference between pixels. Highest difference occurs at -1, 0 and 1.	E	M	M	L	Y	M
Islam, M.R. ; et al…[39]	2014	Image	Spatial	Cryptography, AES, LSB, PSNR, MSB	Stego-crypto method Double security level	E	M	M	L	Y	M
Prabakaran, G.; et al…[40]	2013	Hybrid	Transform	Discrete Wavelet Transform (DWT) or Integer Wavelet Transform (IWT)	Show robustness against many attacks.	G	H	H	M	Y	H
Huy Nguyen Tien; et al… [41]	2013	Image	Spatial	LSBS, LSBM, LSB-MR	Alteration rate decteases from 0.5 to 0.37 Improved recital, compared to LSBM, in terms of cover image quality and resistance	E	M	M	L	Y	M
Jose, J.A.; et al…. [42]	2013	Video	Spatial	Video Motion, Bit stream, Histogram, Uncompressed video	Creates steganographic alteration at the preferred level Insertion by verdict a appropriate candidate vector	E	M	M	L	Y	M
Bedwal, T.; et al… [43]	2013	Image	Spatial	RGB, LSB, Matching, Substitution	Hide RGB image into another RGB image. Use the concept of LSB insertion technique Use of less number of least significant bits makes image quality better.	E	M	M	L	Y	M
Iranpour, M.[44]	2013	Image	Spatial	Hamiltonian path, LSB, MSE	Produce least distortion	E	M	M	L	Y	M
Zaghbani, S.; Rhouma , R. [45]	2013	Image	Spatial	Watermarking, cryptography, chaotic map	maximizing the number of embedded bits in each embedding zone	E	M	M	L	Y	M
Yang Xiaoyuan; er at… [46]	2013	Image	Transform	(STCs), (ML-STCs), DWT, (HVS), ILWT	high security against steganalysis in space and wavelet domain	E	H	H	M	Y	H
Dae-Soo Kim; er at… [47]	2013	Image	Spatial	Gradient-adjusted prediction (GAP), PSNR, Db	The image quality of the projected method is increased by approximately 7 dB in comparison to Niet al's scheme.	E	M	M	L	Y	M

Linlin Zhang; er at…[48]	2013	Image	Spatial	Adaptive steganography,	Stumpy sparsity blocks have higher precedence to communicate clandestine information Improved anti-detection recital	E	M	M	L	Y	M
Cogranne, R.; er at… [49]	2013	Video	Spatial	XOR, 8-bit binary	Frame of clandestine video are broken into components. Each broken component is converted into 8-bit binary values and encrypted using XOR with secret key. Using LSB methods encrypted frames are inserted in the LSB of each frame. Security level doubled.	E	M	M	L	Y	M
Iranpour, M. ;er at…[50]	2013	Image	Spatial	LSB Matching, RS steganalytic algorithm, Grayscale data	The cover image is first divided into some blocks such that each block contains three pixels. Three bits of secret data are then embedded into each block by increasing/decreasing one pixel or rarely three pixels by one as done in LSB matching. Rate of change decreased from 0.50 to 0.375 on average	E	M	M	L	Y	M
Ibaida, A. ;er at… [51]	2013	Image	Transform	ECG, Distortion, point-of-care (POC)	Patient record remain secure ECG remains diagnosable after watermark.	E	H	H	M	Y	H
Biswas, R. ; er at… [52]	2013	Image	Transform	Discrete Cosine Transform (DCT), 8×8 quantized DCT Coefficient (QDC)	The variable bit operation is applied to the proper QDCs to embed a byte of secret data variable bit operation is dependent on the pixel value	E	H	H	M	Y	H
Thanikaisel van, V. ; er at…[53]	2013	Image	Transform	Integer Haar wavelet transform	Reversible Integer Haar wavelet transform is performed on to the red, green and blue components disjointedly Random selection of wavelet coefficients is based on the graph theory Use three keys for embedding, extraction and selection the number of bits to per pixel to hide data.	E	H	H	M	Y	H
Tayel, M.; er at… [54]	2013	Image	Hybrid	Chaos - Fuzzy-Thresholding (CFT)., an inverse ICFT, Thresholding, Fuzzy	Higher degree of security level due to hybrid approach. Use inverse chaotic fuzzy thresholding	E	H	H	M	Y	H
Sidhik, S. ; er at… [55]	2013	Image	Transform	Wavelet Transform, PSNR, MSE	Use of wavelet fusion Robust against attacks	E	H	H	M	Y	H
Tayel, M.B. ; er at… [56]	2013	Image	Hybrid	Cryptography, Hybrid Security message Allocation Algorithm (NHSA), PSNR, MSE	It's a crypto-stego method Double the security level Keep statistical changes minimum	E	H	H	M	Y	H
Hong Cao ; Kot, A.C. [57]	2013	Image	Spatial	edge-adaptive grid (EAG), data carrying pixel locations (DCPL), content adaptive processes (CAP),	dynamic system structure with the redesigned fundamental content adaptive processes performs well against the interferences caused by close-by contours, image noises	E	M	M	L	Y	M

Akhtar, N. ; Johri, P. ; Khan, S.[58]	2013	Image	Spatial	RC4 Algorithm, LSB	good enhancement to Least Significant Bit technique in consideration to security as well as image quality	E	M	M	L	Y	M
Geetha, C.R. ; er at…[59]	2013	Image	Spatial	Minimum Error Replacement [MER], Canny Edge Detector, 2D convolution filter, Dynamic insertion rate	Increase capacity by increasing the number of edge pixels Increase edge pixel by multiple edge detector canny edge detector	E	M	M	L	Y	M
Wei-Jen Wang ; et al… [60]	2013	Image	Spatial	Histogram Shifting, LSB, MSE, PSNR	Apply histogram shifting to increase the capacity	E	M	M	L	Y	M
Iranpour, M.[61]	2013	Image	Spatial	Sobel Operator, Edge Detection, Edge pixel, LSB	Detection of edges is performed by gradient calculation using Sobel operator. As the length of message bit increases, more edges are used to hide data in LSB	E	M	H	L	Y	M
Nadiya, P.V. ; Imran, B.M. [62]	2013	Image	Transform	RSA, DWT, Cryptography, Encryption, Decryption	Double level of data security Crypto-stego model	E	H	H	M	Y	H
Chin-Chen Chang; et al... [63]	2013	Image	Spatial	Dual stego-Image, LSB, dB, Embedding rate, Distortion	Insertion rate is 1.55 bits per pixel Increased capacity does not affect the quality.	E	M	M	L	Y	M
Iranpour, M.[64]	2013	Image	Spatial	(PRNG), Sobel operator, edge detection and adaptive multiple bits substitution	Considerably improve the protection and increase the embedding capacity Use edge region instead of smooth regions	E	M	M	L	Y	M
Yinping Chai ; et al..[65]	2012	Image	Spatial	ECC, Embedding, Extraction,	The projected method is based on Error Correcting code which have an advantage that message can be recovered even some shadows are lost.	E	L	M	M	Y	H
Janakiraman, S; et al…[66]	2012	Image	Spatial	MSB, Segmentation, Bit Plane	The projected method employ the block based segmentation to varied the embedding of secret data. The capacity rate is two or three bits.	E	H	I	M	Y	H
Narasimmalou, T. ; et al…[67]	2012	Image	Transform	DWT, PSNR, Bit Plane	The method uses three levels wavelet decomposition. 4x4 blocks with swapping and one bit plane is taking for processing. Second method uses single wavelet for decomposition.	E	H	M	M	Y	H
Banoci, V. ; et al…[68]	2012	Image	Transform	DCT, Histogram, AES, Encryption, 128-bit Cipher	Embedding is carry out in DCT domain. Hiding a secret data depend on the modification of chosen quantized DCT transform coefficients according to modulo function	E	H	M	M	Y	M

Chang Wang .; et al…[69]	2012	Image	Transform	DCT,STC, Flipping, Steganalysis, Rounding Error,	The STC gives several elucidations to embed messages to a block of coefficients. The projected method determines the best one with minimal distortion effect.	E	H	I	M	Y	H
Mare, S.F,; et al…[70]	2012	Image	Spatial	LSB, Mapping, Embedding Solution	Based on the original smart LSB pixel mapping and data rearrangement design. Due to logical visual and statistical imperceptibility, this is a stronger steganographic model.	E	M	I	M	Y	H
Rong-Jian Chen ; et al…[71]	2012	Image	Spatial	MER, LSB, MEE, K-LSB, Chi-square, Multi-bit	Use the multi bit adaptive insertion and flexible bit location resulting in large embedding capacity and good experimental results.	E	M	I	M	Y	M
Cheng-Ta Huang , et al…[72]	2012	Image	Spatial	VQ, LSB, PSNR	Based on VQ. Uses LSB method to embed data inside another medium. Method is so good that it cannot be detected by well known steganlysis tools.	E	L	M	M	Y	H
Wien Hong ; et al…[73]	2012	Image	Spatial	PPM, EMD, DE, OPAP, bpp	Uses pair of pixel as reference coordinate. Search a coordinate in the neighborhood of the pixel according to a given message digit.	E	M	I	M	Y	H
Avinash, K.G. ; er at…[74]	2012	Image	Spatial	FPPD, MSE, PSNR	Employ pixel pairs differencing for embedding. Increase the embedding capacity with good results against many measures.	E	M	I	M	Y	M
Qiangfu Zhao ; et al…[75]	2012	Image	Spatial	FPS, IGA	Produce facial image by interactive genetic algorithm. Solve the problem more efficiently.	G	H	M	M	Y	M
Hamid, N.; et al...[76]	2012	Image	Transform	SURF, WTC, Content Based, Robust region	Region based stego-scheme. Robust region is selected using speed-up-robust-feature.	E	H	I	M	Y	H
Chin-Feng Lee ; et al …[77]	2012	Image	Spatial	EMD, bpp, dB	Projected method is an extension of EMD. Integrated with image interpolation for making image reversible.	E	H	I	M	Y	M
Wei Sun ; et al…[78]	2012	Audio	Transform	A2IWT, VQ	Transformation of audio signal to image and after embedding image to audio signal is performed. Audio signal to image conversion is done by using re-sampling coefficient and wavelet transform. Embedding is performed using VQ.	E	H	M	M	Y	M
Sengupta, M. ; et al…[79]	2011	Image	Hybrid	DCT, SADCT, MSE, SD, PSNR, IF, IAFDDFTT, SAWT	8x8 masks transform image into time domain. Hash function and a secret key embed the data in the blue component of the RGB of cover image in spatial domain.	E	H	M	M	Y	M

Mare, S.F. ; et al…[80]	2011	Image	Spatial	AES, RSA	It is a crypto-stego scheme. Three techniques are combined together. Two cryptography methods, AES and RSA, are used to encrypt message and the steganography is applied.	E	H	M	M	Y	H
Behbahani, Y.M. ; et al…[81]	2011	Image	Transform	DCT, LSB, SPAM, JPEG	Use Eigen value to make subdivision of quantized DCT matrix coefficient.	E	H	M	M	Y	H
Feng Pan ; et al…[82]	2011	Image	Transform	HVS, Embedding impact, Syndrome Trellis code frequency, Luminance, Texture	Present a distortion function for minimizing impact of embedding in DCT domain.	E	H	I	M	Y	H
Hussain, M. ; et al ...[83]	2011	Image	Spatial	MSE, PSNR, Segmentation	Data hiding is performed in the edge boundary of the object.	E	M	M	M	Y	H
Yung-Yi Lin ; et al…[84]	2011	Image	Spatial	K-bit, power of two Galois field	Invertible secret image shearing technique. Divide input image into multiple sections that fits into alpha-bit space.	E	H	M	M	Y	H
Ghoshal, N. ; et al…[85]	2011	Image	Transform	DFT, Mask, IDFT, DCT, QFT, SCDFT, IDFT	The DFT is applied on the mask of size 2x2. Inverse DFT is performed after embedding to transform it into spatial domain.	E	H	M	M	Y	H
Guangjie Liu ; et al… [86]	2011	Image	Spatial	Correlation	2x4 block size is used as a cover unit. Local correlation of the block determines the number of secret message bits to be embedded.	E	H	M	M	Y	H
Yan-ping Zhang ; et al… [87]	2011	Image	Spatial	Hamming Code, Wet Paper codes	Uses Hamming code and wet paper codes to hide seven bits into a group of seven cover pixel at a time. If Embedding of seven bits is not successful then three bits are embedded.	E	M	I	M	Y	H

Nasab, S.E. ; et al…[88]	2011	Image	Transform	LSB, 2D, int2int, ALE, Steganalysis, 8x 8 mask, DWT	Use 2D int2int wavelet transform and Raman's idea for hiding secret data. 8x8 mask and bit planes are created. Caw aguish compute the complexity and capacity of each block.	E	H	I	M	Y	H
Sengupta, M. ; et al… [89]	2011	Image	Transform	DCT, AINCDCT, MSE, PSNR, IF	Transformation of cover image into spectral domain by 2x2 masks is applied. Replacement of message bit is performed by hash function and secret key.	E	H	M	M	Y	H
Bobate, R.V. ; et al… [90]	2011	Image	Spatial	LSB, 24 bit, Hue	Message bits are embedded in higher LSB layer.	E	M	M	M	Y	H
Chung-Li Hou ; et al… [91]	2011	Image	Spatial	Parity Checker	Use tree based parity check scheme for hiding secret message and creates least distortion.	E	M	M	L	Y	H
Banoci, V. ; et al…[92]	2011	Image	Transform	DWT	Presented method is grayscale image hiding scheme. Concealment is performed in DWT domain by changing the coefficient.	E	H	M	M	Y	H
Mandal, J.K. ; et al… [93]	2011	Image	Spatial	DHPVD, PSNR, IF	Bit concealment is performed in both the edge and smooth area. Bit handling minimizes the difference between cover and stego pixels.	E	M	I	M	Y	H
Mohan, M. ; et al… [94]	2011	Image	Transform	LSB, PSNR, ASCII	It is a crypto-stegio model. Use contour let transform for the concealment of encrypted data.	E	H	M	M	Y	H
Nugraha, R.M. et al… [95]	2011	Audio	Spatial	Spread Spectrum	Embedding is performed by using Sequence Spread Spectrum Embedded data will be heard as noise.	E	H	M	M	Y	H

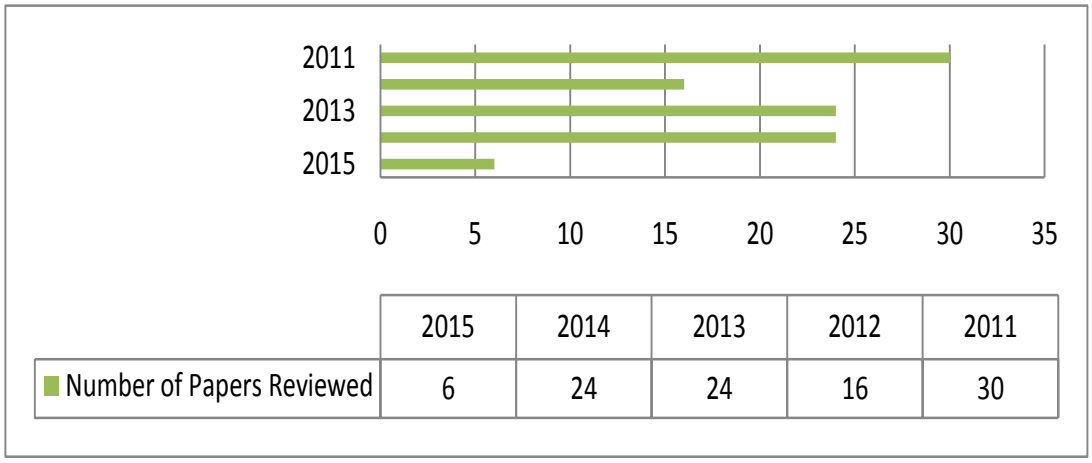
Pramitha, K. ; et al…[96]	2011	Image	Spatial	RSA	It's a stego-crypto model. Encryption is performed by using RSA algorithm.	E	H	M	M	Y	H
Hui-Yu Huang ; et al … [97]	2011	Image	Transform	DWT, 2-D DWT	Projected method is based on quantized coefficient of DWT in frequency domain.	G	H	I	M	Y	H
Shiva Kumar, K.B. ; et al…[98]	2011	Image	Transform	DTTRS, DWT, IWT, PSNR	On each segmented 4x4 block DWT is applied and then IWT is applied which makes it more complex.	E	H	I	M	Y	H
Chen Gouxi ; et al… [99]	2011	Image	Spatial	F5, Morphology, Reconstruction	Algorithm is based on edge processing. F5 method is used to embed the message bit.	E	M	I	M	Y	H
Guoqi Luo ; et al… [100]	2011	Image	Spatial	Cochin's Security, Kulback Libeler (KL)	While embedding it change the order of pixels rather than modifying their value.	E	M	M	L	Y	M
Al-Ataby, A.A. ; et al… [101]	2011	Image	Transform	Curve let Transform	Method uses curve let transform that reduces the distortion.	E	H	M	H	Y	H
Meenpal, T. ; et al…[102]	2011	Image	Transform	IWT, LSB, CFD, Threshold	Uses two LSBs of higher frequency CFD (2, 2) integer wavelet whose magnitude are smaller than a predefined threshold.	E	H	I	M	Y	H
Katiyar, S. ; et al… [103]	2011	Image	Spatial	Cryptography	It is a crypto-stego model. Provide biometric and password security to vote account. Image is used as cover object for steganography and key for cryptography.	E	H	M	M	Y	H

Bajwa, I.S.; et al… [104]	2011	Image	Spatial	Hash Function	Use the hash function for concealment of secret message in grayscale image.	E	M	M	L	Y	H
Saha, A. ; et al … [105]	2011	Image	Spatial	24-bit bitmap, LSB	Most frequent occurring pixel is used for data hiding. LSB method is applied on those pixels.	E	L	M	L	Y	M
Mandal, J.K. ; et al… [106]	2011	Image	Transform	DFT, GASFD	2x2 mask of the image is transformed from frequency domain to spatial domain after embedding. Genetic algorithm is used to enhance the security.	E	H	M	M	Y	H
Khosravi, M.J. ; et al … [107]	2011	Image	Transform	IWT, Fletcher 16-Checksum	Shares and Fletcher 16- checksum of share are embedded in cover medium using IWT.	E	H	M	M	Y	H
Dutta, A.; et al…[108]	2011	Image	Spatial	LSB, LSB+3, Encryption, Decryption	It's a crypto-stego model. Message bits are encrypted using simple bit exchange method. For steganography, LSB and LSB+3 bits are changed.	E	M	M	L	Y	H

LSB: Least Significant Bit, GLM: Gray Level Modification, MSE: Mean Square Error, PSNR: Peak Signal to Noise Ratio, SC: Structural Content, AD: Average Difference, MD: Maximum Difference, NAE: Normalized Absolute Error, HVS: Human Visual System, LTP: Local Texture Pattern, TS: Texture Synthesis, VQ: Vector quantization, UIQI: Universal Image Quality Index, SSIM: Structural Similarity Index Measure, ROI: Region of Interest, RGB: Red Green Blue, YCbCr: Colour Model, MBS: Module Based Substitution, DCT: Discrete Cosine Transformation, PFM: Pixel Factor Mapping, JPEG: Joint Photographic Expert Group, DWT: Discrete Wavelet Transform, RDH: Reversible Data Hiding, PVD: Pixel Value Differencing, ME: Matrix Embedding, PRNG: Pseudorandom Number Generator, BER: Bit Error Rate, CNP: Card Not Present, LSBR: Least Significant Bit Replacement, OPAP: Optimal Pixel Adjustment Process, PDHS: Pixel Difference Histogram Shifting, MSB: Most Significant Bit, IWT: Integer Wavelet Transform, LSBS: Least Significant Bit Substitution, LSBM: Least Significant Bit Matching, LSB-MR: Least Significant Bit Matching Revisited, STC: Syndrome Trellis Codes, ML-STC: Multi-Layered Syndrome Trellis Codes, GAP: Gradient Adjusted Prediction, dB: Decibel, XOR: Exclusive OR, RS: Regular Singular, ECG: Electrocardiograph, POC: Point of Care, QDC: Quantized DC, CFT: Chaos Fuzzy Thresholding, ICFT: Inverse Chaos Fuzzy Thresholding, NHSA: New Hybrid Security Message Allocation Algorithm, EAG: Edge Adaptive Grid, DCPL: Data Carrying Pixel Locations, CAP: Content Adaptive Processes, MER: Minimum Error Replacement, ECC: Error Correction Code, MSB: Most Significant Bit, STC: Syndrome Trellis Coding, MEE: Minimum Embedding Error, VQ: Vector Quantization, PPM: Pixel Pair Matching, EMD: Exploring Modification Direction, DE: Diamond Encoding, bpp: Bit Per Pixel, FPPD: Five Pixel Pair Differencing, FPS: Feature Point Set, IGA: Interactive Genetic Algorithm, SURF: Speeded-Up Robust Feature, SADCT: Self Authentication of Colour image through DCT, SD: Standard Deviation, AES: Advance Encryption Standards, SPAM: Subtractive Pixel Adjacency Matrix, JPEG: Joint Photographic Expert Group, DFT: Discrete Cosine Transformation, IDFT: Inverse DCT, QFT: Quantized Fourier Transformation, SCDFT: Spatio Chromatic DFT, ALE: Amplitude of Histogram Local Extrema, AINCDCT: Authentication of image through non convoluted DCT, IF: Image Fidelity, DHPVD: Data Hiding Scheme for Digital Image, ASCII: American Standard Code for Information Interchange, RSA: Rivest, Shamir and Adleman, DTTRS: Dual Transform Technique for Robust steganography, KL: Kullback-Liebler, DFT: Discrete Fourier Transform, GASFD: Genetic Algorithm based Steganography in Frequency Domain.

3. Results and Discussion

Figure 1 shows the graph of number of paper selected for review. Maximum publications have been selected from the year 2011 and minimum are from the year 2015. Graph shows that this topic of research is a sound field throughout the selected years.
Figure 2 shows the graph of classification of yearly selected paper into Spatial, Transform and hybrid approach. It is clear from the graph that maximum contribution is of spatial classification. Transform domain is on second and very less work having been done and published in hybrid domain. Figure 3 shows the yearly percentage of selected paper for spatial domain. Among the selected papers the maximum contribution was recorded from 2014 with 29%, followed by 25% from 2011, 24% from 2013, 13% from 2012 and 9% from 2015. Figure 4 shows the yearly percentage of selected paper for transform domain. Among the selected papers the maximum contribution was recorded from 2011 with 42%, followed by 24% from 2013, 17% from 2014, 17% from 2012 and 0% from 2015.



	2015	2014	2013	2012	2011
Number of Papers Reviewed	6	24	24	16	30

Figure 1. Graph of Number of Papers Reviewed

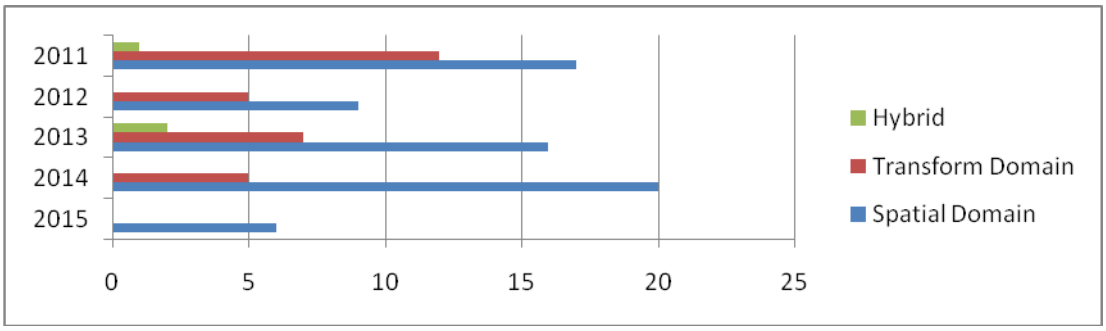


Figure 2. Graph of Domain Classification of Papers Reviewed

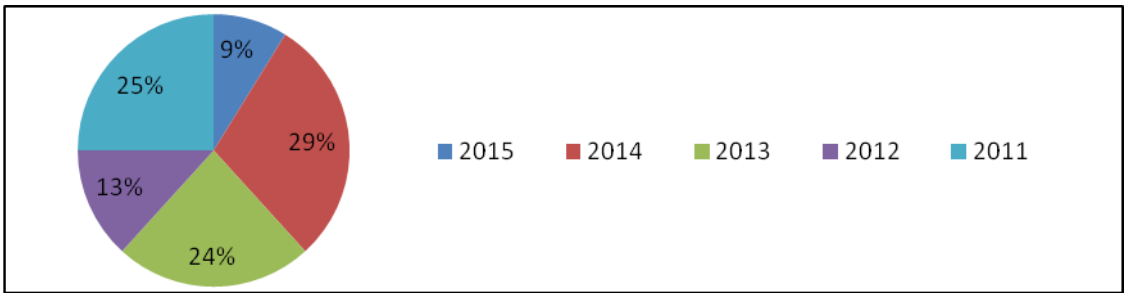


Figure 3. Graph of Spatial Domain Methods used in Papers Reviewed

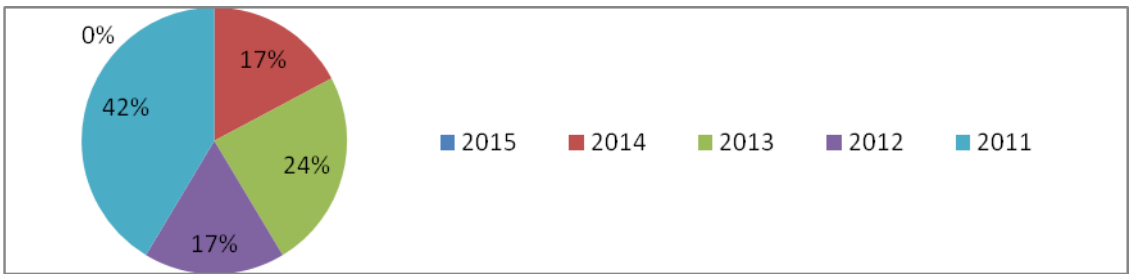


Figure 4. Graph of Transform Domain Method used in Papers Reviewed

Figure 5 shows the yearly percentage of selected paper for hybrid domain. Among the selected papers the maximum contribution was recorded from 2013 with 67%, followed by 33% from 2011, 0% from 2013, 0% from 2012 and 0% from 2015.

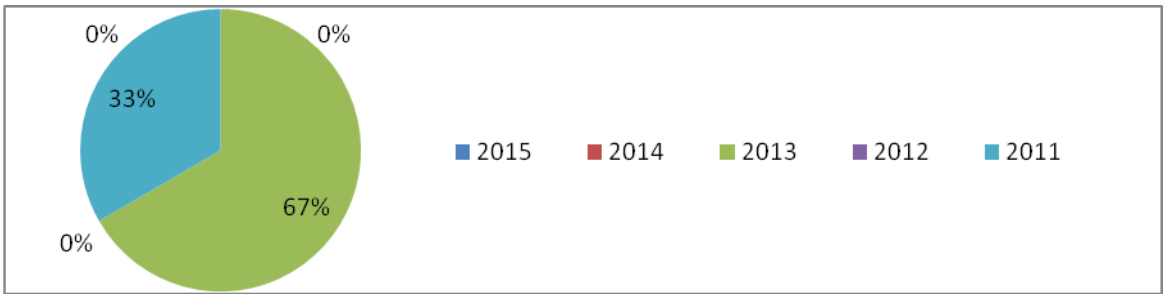


Figure 5. Graph of Hybrid Domain Method used in Papers Reviewed

Figure 6 shows the graph of classification of yearly selected papers based on the type of medium used as cover object. It is clear from the Figure 7 that in the selected years, maximum contributions uses image as cover object.

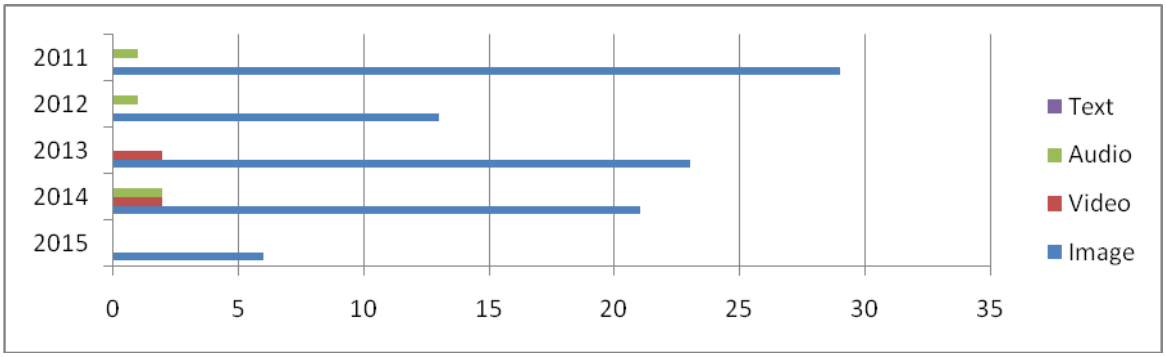


Figure 6. Graph of Medium used in Papers Reviewed

Figure7 shows the yearly percentage selected paper for steganography method that uses image as medium for hiding the secret data. Among the selected papers the maximum contribution was recorded from 2011 with 31%, followed by 25% from 2013, 23% from 2014, 14% from 2012 and 7% from 2015.

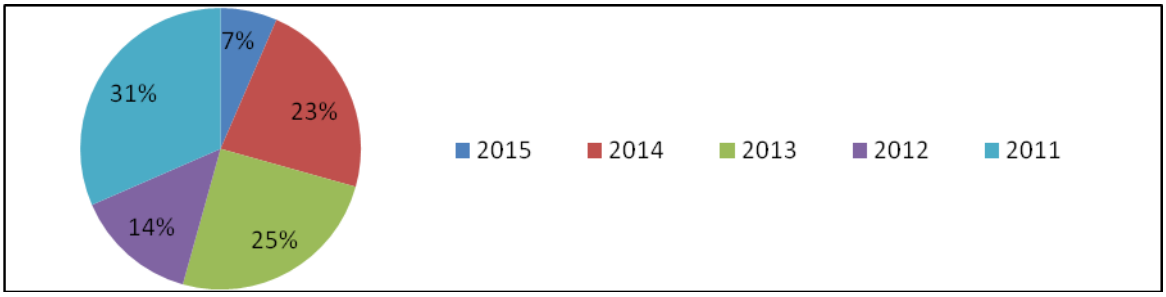


Figure 7. Graph of Image as Medium used in Papers Reviewed

Figure 8 shows the yearly percentage selected paper for steganography method that uses video file as medium for hiding the secret data. Among the selected papers the maximum contribution was recorded from 2011 with 88%, followed by 6% from 2014, 6% from 2013, 0% from 2012 and 0% from 2015.

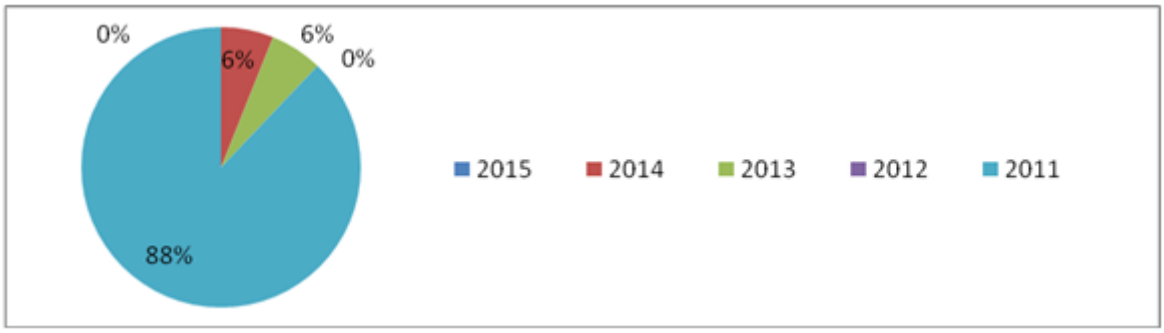


Figure 8. Graph of Video as Medium used in Papers Reviewed

Figure 9 shows the yearly percentage selected paper for steganography method that uses audio file as medium for hiding the secret data. Among the selected papers the maximum contribution was recorded from 2014 with 50%, followed by 25% from 2011, 25% from 2012, 0% from 2013 and 9% from 2015.

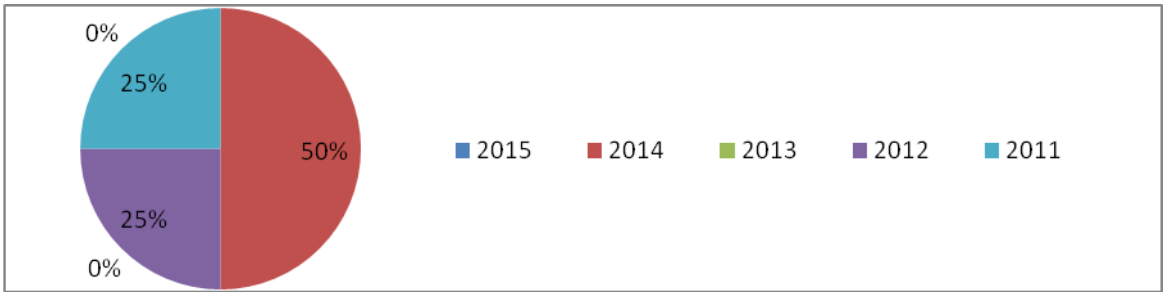


Figure 9. Graph of Audio as Medium used in Papers Reviewed

For the papers of selected years no paper uses the steganography method that uses text file as medium for hiding the secret data.

4. Conclusions and Future Work

This paper presents the review of 100 papers of the recent years. Review is based on the type of medium used as cover object, domain of stego method and important measures for a good stego scheme. The critical analysis, results and discussion shows that the topic of research sounds excellent in the recent years. Mostly the methods are projected in spatial domain and image is used as cover medium. The reason of spatial domain method is that its complexity is less as compare to that of transform and hybrid approach. And images are widely used because of the reason that its size is less as compare to that of audio or video file. In images, the greyscale image takes less space and transmission time and bandwidth as compare to that of colour images. But both, greyscale and colour, images are popular and used for data hiding. As this field of research is a sound topic and gaining importance rapidly, this detail and comprehensive review will be a best tool for quick understanding the recent projected techniques and will help to present the new and better methodology. Future contribution will focus on the experimental review of steganographic schemes.

Acknowledgement

We are very thankful to **Sir Dr. Malik Muhammad Saad Missen**, Director of Weekend Program at the Department of CS&IT, Islamia University of Bahawalpur, Pakistan, and **Sir Dr. Nadeem Salamat**, Associate Professor at the Department of Basic Sciences, Khwaja Freed Information Technology University, R.Y.Khan, Pakistan, for help.

References

[1] R. M. Khurrum, S. Ndeem, M. Saad and R. Aqsa, "Robust Increased Capacity Image Steganograpgy Scheme", International Journal of Advanced Computer Science and Applications, vol. 5, no. 11, **(2014)**, pp. 125-131.

[2] R. Aqsa, M. Muhammad, M. Saas and S. Nadwwm, "Analysis of Steganography Technique using Least Significant Bit in Graysclae Images and their ectension to Colour Images", Journal of Scientific Research and Report, vol. 9, no. 3, **(2016)**, pp. 1-14.

[3] R. Aqsa and R. M. Khurrum, "Experimental Review of Steganography Method that uses 5^{th}, 6^{th} and 7^{th} Bit of a Pixel", International Journal of Computer Applications, vol. 121, no. 1, **(2015)**, pp. 41-45.

[4] R. Aqsa and R. M. Khurrum, "Experimental Analysis and Review of "Increased Capacity of Information Hinding" , International Journal of Security and its Applications, vol. 9, no. 12, **(2015)**, pp. 221-230.

[5] R. Aqsa and R. M. Khurrum, "Experimental Review of "Grey Level Modification", Steganography, International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, no. 11, **(2015)**, pp. 256-272.

[6] R. Aqsa and M. K. Rahim, "Stego-Scheme for Secret Communication in Grayscale and RGB Images", British Journal of Mathematics and Computer Science, vol. 10, no. 1, **(2015)**, pp. 1-9.

[7] R. Aqsa, "Experimental Analysis and Comparison of LSB substitution and LSB Matching Method of Information Security", IJCSI International Journal of Computer Science Issues, vol. 12, no. 1, **(2015)**, pp. 91-100.

[8] R. M. Khurrum, R. Aqsa, S. Nadeem and M. Saad, "Experimental Analysis of Matching Technique of Steganograph for Greyscale and Colour Image", International Journal of Computer Science & Information Technology (IJCSIT), vol. 6, no. 6, **(2014)**, pp. 157-166.

[9] A. Rashid, "Robust Electronic communication Scheme in Spatial Domain", British Journal of Mathematics and Computer Science, vol. 7, no. 3, **(2015)**, pp. 218-228.

[10] D. Debnath, S. Deb and N. Kar, "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher & RGB Image Steganography", Computational Intelligence and Networks (CINE), **(2015)**, pp. 178 – 183.

[11] B. Feng, W. Lu and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", Information Forensics and Security, IEEE Transactions, vol. 10, **(2015)**, pp. 243 – 255.

[12] M. Nosrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm", Advanced Computing & Communication Technologies (ACCT), **(2015)**, pp. 102 – 107.
[13] K. Wu and C. Wang, "Steganography Using Reversible Texture Synthesis", vol. 24, no. 1, **(2015)**, pp. 130 – 139.
[14] Z. Pan, X. Ma and X. Deng, "New reversible full-embeddable information hiding method for vector quantisation indices based on locally adaptive complete coding list", Image Processing, IET ,vol. 9, no. 1, **(2015)**, pp. 22 – 30.
[15] M. Khurrum, R. Rashid, N. Salamat, S. Missen and A. Rashid, "Robust Increased Capacity Image Steganographic Scheme", International Journal of Advanced Computer Science and Applications (IJACSA), vol. 5, no. 11, **(2014)**.
[16] S. Khupse and N. N. Patil, "An adaptive steganography technique for videos using Steganoflage", Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference, **(2014)**.
[17] N. Akhtar, A. Bano and F. Islam, "An Improved Module Based Substitution SteganographyMethod, Communication Systems and Network Technologies (CSNT)", Fourth International Conference, **(2014)**.
[18] I. Banerjee, S. Bhattacharyya, G. Sanyal, "Robust image steganography with pixel factor mapping (PFM) technique", Computing for Sustainable Global Development (INDIACom), International Conference, **(2014)**.
[19] S. Goswami, J. Goswami and R. Mehra, "An efficient algorithm of steganography using JPEG colored image", Recent Advances and Innovations in Engineering (ICRAIE), **(2014)**.
[20] N. Gupta and N. Sharma, "Dwt and Lsb based Audio Steganography Optimization, Reliabilty, and Information Technology (ICROIT)", **(2014)**.
[21] K. A. Darabkh, I. F. Jafar, R. T. Al-Zubi and M. Hawa, "An improved image least significant bit replacement method", Information and Communication Technology, Electronics and Microelectronics (MIPRO), **(2014)**.
[22] V. Senthooran and L. Ranathunga, "DCT coefficient dependent quantization table modification steganographic algorithm, Networks & Soft Computing (ICNSC)", **(2014)**.
[23] T. S. K. Shripriyadharshini, S. Yohalakshmi and S. Deepa, "Reserve Room based Reversible Data Hiding in digital images, Communications and Signal Processing (ICCSP)", **(2014)**, pp. 1452 – 1456.
[24] Chou, Y. Chen, G. Huang, H. Lee, H. Ching and K. J. Lin, "A Reversible Data Hiding Method Using Inverse S-Scan Order and Histogram Shifting", Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), **(2014)**.
[25] H. Al-Dmour, A. Al-Ani and H. Nguyen, "An efficient steganography method for hiding patient confidential information, Engineering in Medicine and Biology Society (EMBC), **(2014)**, pp. 222 – 225.
[26] S. Sarreshtedari and M. A. Akhaee, "One-third probability embedding: a new ±1 histogram compensating image least significant bit steganographyscheme", Image Processing, IET , vol. 8, no. 2, **(2014)**, pp. 78 – 89.
[27] R. Roy and S. Changder, "Image steganography with block entropy based segmentation and variable rate embedding", Business and Information Management (ICBIM), **(2014)**, pp. 75 – 80.
[28] C.-Y. Lin, K.-R. Chen, J.-J. Wang, "A Steganographic Method for Binary Embedding Using Time-Varying Convolutional Codes", Computer, Consumer and Control (IS3C), **(2014)**, pp. 1221 – 1224.
[29] H. B. Dieu and N. X. Huy, "An improved technique for hiding data in audio", Digital Information and Communication Technology and it's Applications (DICTAP), **(2014)**, pp. 149 – 153.
[30] J. M. G. Cardenas, "Secret Key Steganography with Message Obfuscation by Pseudo-random Number Generators", Computer Software and Applications Conference Workshops (COMPSACW), **(2014)**, pp. 164 – 168.
[31] L. Kedmenec, A. Poljicak and L. Mandic, "Copyright protection of images on a social network", ELMAR (ELMAR), **(2014)**, pp. 1 – 4.
[32] H. Yajam, M. Allah, A. Sadat and M. Amirmazlaghani, "A new linguistic steganography scheme based on lexical substitution", Information Security and Cryptology (ISCISC), **(2014)**, pp. 155 – 160.
[33] A. Bidokhti and S. Ghaemmaghami, "Wet paper coding", Information Security and Cryptology (ISCISC), **(2014)**, pp. 210 – 213.
[34] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography, Electrical", Electronics and Computer Science (SCEECS), **(2014)**, pp. 1–5.
[35] Kumar, S. ; Gupta, A. ; Chandwani, A. ; Yadav, G. ; Swarnkar, R. , RGB image watermarking on video frames using DWT,Confluence The Next Generation Information Technology Summit (Confluence), 2014, Page(s): 675 – 680, DOI: 10.1109/CONFLUENCE.2014.6949263
[36] Gupta,P.K. ; Roy,R. ; Changder,S.,Asecure image steganography technique with moderately higher significant bit embedding, Computer Communication and Informatics (ICCCI), 2014, Page(s):1–6,DOI: 10.1109/ICCCI.2014.6921726
[37] Mandal, Ashis Kumar ; Kaosar, Mohammed ; Islam, Md.Olioul ;Hossain, Md.Delowar, An approach for enhancing message security in audiosteganography, Computer and Information Technology (ICCIT), 2013, Page(s): 383 – 388, DOI: 10.1109/ICCITechn.2014.6997310

[38] Chou, Yung Chen ; Lee, Huang Ching ; Yu, Yong Jin ,A Novel Reversible Data Hiding Scheme Using Ripple Strategy and Histogram Shifting, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014, Page(s): 138 – 141, DOI: 10.1109/IIH-MSP.2014.41
[39] Islam, M.R. ; Siddiqa, A. ; Uddin, M.P. ; Mandal, A.K. ; Hossain, M.D. ,An efficient filtering based approach improving LSB imagesteganography using status bit along with AES cryptography, Informatics, Electronics & Vision (ICIEV),2014,Page(s):1–6, DOI: 10.1109/ICIEV.2014.6850714
[40] Prabakaran, G. ; Bhavani, R. ; Kanimozhi, K. , Dual transform based steganography using wavelet families and statistical methods, Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 , Page(s): 287 - 293 ,DOI: 10.1109/ICPRIME.2013.6496488
[41] Huy Nguyen Tien ; Bac Le, Noise reduction approach for LSB matching revisited, Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2013 , Page(s): 76 – 79, DOI: 10.1109/RIVF.2013.6719870
[42] Jose, J.A. ; Titus, G., Data hiding using motion histogram, Computer Communication and Informatics (ICCCI), 2013, Page(s): 1 - 4 , DOI: 10.1109/ICCCI.2013.6466269
[43] Bedwal, T. ; Kumar, M. , An enhanced and secure image steganographic technique using RGB-box mapping, Confluence 2013: The Next Generation Information Technology Summit, Page(s): 385 – 393, DOI: 10.1049/cp.2013.2347
[44] Iranpour, M. .LSB-Based Steganography Using Hamiltonian Path, Intelligent Information Hiding and Multimedia Signal Processing, 2013, Page(s): 586 – 589, DOI: 10.1109/IIH-MSP.2013.151
[45] Zaghbani, S. ; Rhouma, R., Data hiding in spatial domain image using chaotic map, Modeling, Simulation and Applied Optimization (ICMSAO), 2013, Page(s): 1 – 5, DOI: 10.1109/ICMSAO.2013.6552626
[46] Yang Xiaoyuan ; Guo Duntao ; Li Jun , An image steganography based on Multi-Layered Syndrome-Trellis Codes in DWT domain, Control Conference (CCC),2013,Page(s): 3738 – 3743
[47] Dae-Soo Kim ; Gil-Je Lee ; Kee-Young Yoo , Reversible Image Hiding Scheme for High Quality Based on Histogram Shifting, Information Technology: New Generations (ITNG), 2013, Page(s): 392 – 397, DOI: 10.1109/ITNG.2013.61
[48] Linlin Zhang ; Jianjun Wang, Adaptive information hiding based on local sparsity, Information Management, Innovation Management and Industrial Engineering(ICIII),2013,Volume:2,Page(s):273–2777, DOI: 10.1109/ICIII.2013.6703137
[49] Cogranne, R. ; Thanh Hai Thai ; Retraint, F.,Asymptotically optimal detection of LSB matching data hiding, Image Processing (ICIP), 2013, Page(s): 4437 – 4441,DOI: 10.1109/ICIP.2013.6738914
[50] Iranpour, M. ; Farokhian, F.,Minimal distortion steganography using well-defined functions, High Capacity Optical Networks and Enabling Technologies (HONET-CNS), 2013, Page(s): 21 – 24, DOI: 10.1109/HONET.2013.6729751
[51] Ibaida, A. ; Khalil, I. , Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems, Biomedical Engineering, Volume: 60 , Issue: 12 , Page(s): 3322 – 3330, DOI: 10.1109/TBME.2013.2264539
[52] Biswas, R. ; Mukherjee, S. ; Bandyopadhyay, S.K. , DCT Domain Encryption in LSB Steganography, Computational Intelligence and Communication Networks (CICN), 2013, Page(s): 405 – 408, DOI: 10.1109/CICN.2013.89
[53] Thanikaiselvan, V. ; Arulmozhivarman, P. ,High security image steganography using IWT and graph theory, Signal and Image Processing Applications (ICSIPA), 2013, Page(s): 337 – 342, DOI: 10.1109/ICSIPA.2013.6708029
[54] Tayel, M. ; Shawky, H. ; Hafez, A.E.S., A hybrid chaos- fuzzy -threshold steganography algorithm for hiding secure data, Advanced Communication Technology (ICACT), 2013, Page(s): 156 – 161
[55] Sidhik, S.; Sudheer, S.K.; Mahadhevan Pillsai, V.P., Modified high capacity steganography for color images using wavelet fusion, Fiber Optics in Access Network (FOAN), 2013, 40 – 43, DOI: 10.1109/FOAN.2013.6648824
[56] Tayel, M.B. ; Sayed Hafez, A.E.-D. ; Zied, H.S., A new hybrid security allocation steganography algorithm, Computer Engineering & Systems (ICCES), 2013, 217-220, DOI: 10.1109/ICCES.2013.6707207
[57] Hong Cao; Kot, A.C., On Establishing Edge Adaptive Grid for Bilevel Image Data Hiding, Information Forensics and Security, Volume: 8 , Issue: 9, 1508-1518, DOI: 10.1109/TIFS.2013.2274041
[58] Akhtar, N. ; Johri, P. ; Khan, S. , Enhancing the Security and Quality of LSB Based Image Steganography, Computational Intelligence and Communication Networks (CICN), 385-390, DOI: 10.1109/CICN.2013.85
[59] Geetha, C.R. ; Basavaraju, S. ; Puttamadappa, C. , Variable load image steganography using multiple edge detection and minimum error replacement method, Information & Communication Technologies (ICT), 53-58, DOI: 10.1109/CICT.2013.6558061
[60] Wei-Jen Wang ; Yu-Hong Zhang ; Cheng-Ta Huang ; Shiuh-Jeng Wang , Steganography of Data Embedding in Multimedia Images Using Interpolation and Histogram Shifting, Intelligent Information Hiding and Multimedia Signal Processing, 2013, 387-390, DOI: 10.1109/IIH-MSP.2013.103

[61] Iranpour, M., Adaptive edge tracing steganography, ELMAR, 2013 , 27 - 30
[62] Nadiya, P.V. ; Imran, B.M. , Image steganography in DWT domain using double-stegging with RSA encryption, Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 , 283-287 ,DOI: 10.1109/ICSIPR.2013.6497941
[63] Chin-Chen Chang; Tzu-Chuen Lu; Gwoboa Horng ; Ying-Hsuan Huang ; Yung-Ming Hsu , A high payload data embedding scheme using dual stego-images with reversibility, Information, Communications and Signal Processing (ICICS) 2013, 1-5, DOI: 10.1109/ICICS.2013.6782790
[64] Iranpour, M. , A novel steganographic method based on edge detection and adaptive multiple bits substitution, Digital Signal Processing (DSP), 2013, 1-6, DOI: 10.1109/ICDSP.2013.6622828
[65] Yinping Chai; Kun Zhang; Peng Liu, Shearing Secret Image with Error Correcting Codes, ICT and Energy Efficiency and Workshhop on Information Theory and Security , Publication Year: 2012 , Page(s): 204 – 208, DOI: 10.1049/cp.2012.1892
[66] Janakiraman, S. ; Suriya, N. ; Nithiya, V. ; Radhakrishnan, B. ;Ramanathan, J. ; Amirtharajan, R. , Reflective code for gray block embedding, Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012, Publication Year: 2012 , Page(s): 215 – 220, DOI: 10.1109/ICPRIME.2012.6208346
[67] Narasimmalou, T. ; Joseph, R.A. , Discrete Wavelet Transform based steganography for transmitting images, Advances in Engineering, Science and Management (ICAESM), 2012 Publication Year: 2012 , Page(s): 370 - 375
[68] Banoci, V. ; Bugar, G. ; Levicky, D. ; Klenovicova, Z. ,Histogram secure steganography system in JPEG file on modulus function, RADIOELEKTRONIKA, 2012 , Publication Year: 2012 , Page(s): 1 - 4
[69] Chang Wang ; Jiangqun Ni , An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients, Acoustics, Speech and Signal Processing (ICASSP), 2012 , Page(s): 1785 - 1788 ,DOI: 10.1109/ICASSP.2012.6288246
[70] Mare, S.F. ; Vladutiu, M. ; Prodan, L. , High capacity steganographic algorithm based on payload adaptation and optimization, Applied Computational Intelligence and Informatics (SACI), 2012 , 2012 , Page(s): 87 – 92, DOI: 10.1109/SACI.2012.6249981
[71] Rong-Jian Chen ; Shi-Jinn Horng , Multi-bit Adaptive Embedding Algorithm for Anti-forensic Steganography, Biometrics and Security Technologies (ISBAST), 2012 , 2012 , Page(s): 82 - 89 . ,DOI: 10.1109/ISBAST.2012.29
[72] Cheng-Ta Huang ; Wei-Jen Wang ; Min-Yi Tsai ; Chin-Feng Lee, Employing LSB and VQ for Undetectable Secret Data Hiding, Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012, Page(s): 644 – 649, DOI: 10.1109/UIC-ATC.2012.62
[73] Wien Hong ; Tung-Shou Chen, A Novel Data Embedding Method Using Adaptive Pixel Pair Matching, Information Forensics and Security, Volume: 7 , Issue: 1 , Part: 2 ,2012, Page(s): 176 - 184 , DOI: 10.1109/TIFS.2011.2155062
[74] Avinash, K.G. ; Joshi, M.S. , A Secured Five Pixel Pair Differencing Algorithm for Compressed Image Steganography, Computer and Communication Technology (ICCCT), 2012, Page(s):278–282,DOI: 10.1109/ICCCT.2012.63
[75] Qiangfu Zhao ; Akatsuka, M. ; Cheng-Hsiung Hsieh, Generating facial images for steganography based on IGA and image morphing, Systems, Man, and Cybernetics (SMC),2012,Page(s):364–369,DOI: 10.1109/ICSMC.2012.6377728
[76] Hamid, N. ; Yahya, A. ; Ahmad, R.B. ; Al-Qershi, O. , Characteristic region based image steganography using Speeded-Up Robust Features technique, Future Communication Networks (ICFCN), 2012 , Page(s): 141 - 146 , DOI: 10.1109/ICFCN.2012.6206858
[77] Chin-Feng Lee ; Kai-Chin Chen , Efficient reversible steganographic embedding by the integration of reduplicated EMD and image interpolation, Information Security and Intelligence Control (ISIC), 2012,Page(s):182–185,DOI: 10.1109/ISIC.2012.6449736
[78] Wei Sun ; Rong-Jun Shen ; Fa-Xin Yu ; Zhe-Ming Lu, Data Hiding in Audio Based on Audio-to-Image Wavelet Transform and Vector Quantization, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012, Page(s): 313 – 316, DOI: 10.1109/IIH-MSP.2012.82
[79] Sengupta, M. ; Mandal, J.K. , Self authentication of color images through discrete cosine transformation (SADCT), Recent Trends in Information Technology (ICRTIT), 2011 , Page(s): 832 - 836 ,DOI: 10.1109/ICRTIT.2011.5972304
[80] Mare, S.F. ; Vladutiu, M. ; Prodan, L. , Secret data communication system using steganography, AES and RSA, Design and Technology in Electronic Packaging (SIITME), 2011, Page(s): 339 – 344, DOI: 10.1109/SIITME.2011.6102748
[81] Behbahani, Y.M. ; Ghayour, P. ; Farzaneh, A.H. , Eigenvalue Steganography based on eigen characteristics of quantized DCT matrices,Information Technology and Multimedia (ICIM), 2011 , Page(s): 1 - 4 , DOI: 10.1109/ICIMU.2011.6122769
[82] Feng Pan ; Jun Li ; Xiuguang Li ; Yao Guo , Steganography based on Minimizing Embedding Impact function and HVS, Electronics, Communications and Control (ICECC), 2011, Page(s): 490 - 493 ,DOI: 10.1109/ICECC.2011.6067565

[83] Hussain, M. ; Hussain, M. , Embedding data in edge boundaries with high PSNR, Emerging Technologies (ICET), 2011 , Page(s): 1 - 6 , DOI: 10.1109/ICET.2011.6048469
[84] Yung-Yi Lin ; Ran-Zan Wang , Improved Invertible Secret Image Sharing withSteganography, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, Page(s): 93 – 96, DOI: 10.1109/IIHMSP.2011.58
[85] Ghoshal, N. ; Mandal, J.K. , A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology (ICRTIT), 2011, Page(s): 826 - 831 , DOI: 10.1109/ICRTIT.2011.5972302
[86] Guangjie Liu ; Weiwei Liu ; Yuewei Dai ; Shiguo Lian , An Adaptive Matrix Embedding for Image Steganography, Multimedia Information Networking and Security (MINES), 2011, Page(s): 642 - 646 , DOI: 10.1109/MINES.2011.138
[87] Yan-ping Zhang ; Juan Jiang ; Chao Xu ; Bo Hua ; Xiao-yan Chen, A New Scheme for Information Hiding Based on DigitalImages, Computational Intelligence and Security (CIS), 2011, Page(s): 512 - 516 , DOI: 10.1109/CIS.2011.119
[88] Nasab, S.E. ; Aghaeinia, H. , A new int2int high capacity robust steganography method with LSB 1/3 and rounding method for embedding message, Electrical Engineering (ICEE), 2011, Page(s): 1,
[89] Sengupta, M. ; Mandal, J.K. , Authentication of images through non convoluted DCT (AINCDCT), Communication and Industrial Application (ICCIA), 2011, Page(s): 1 – 4, DOI: 10.1109/ICCIndA.2011.6146672
[90] Bobate, R.V. ; Khobragade, A.S. , Optimal implementation of digital steganography in an true color images for the secrete communication, Advances in Recent Technologies in Communication and Computing (ARTCom 2011), Page(s): 91 – 95, DOI: 10.1049/ic.2011.0057
[91] Chung-Li Hou ; ChangChun Lu ; Shi-Chun Tsai ; Wen-Guey Tzeng , An Optimal Data Hiding Scheme With Tree-Based Parity Check, Image Processing, IEEE , Volume: 20 , Issue: 3 , Page(s): 880 - 886 , DOI: 10.1109/TIP.2010.2072513
[92] Banoci, V. ; Bugar, G. ; Levicky, D. , A novel method of image steganography in DWT domain, Radioelektronika (RADIOELEKTRONIKA), 2011, Page(s): 1 - 4 , DOI: 10.1109/RADIOELEK.2011.5936455
[93] Mandal, J.K. ; Khamrui, A. , A Data-Hiding Scheme for Digital Image Using Pixel Value Differencing (DHPVD), Electronic System Design (ISED), 2011, Page(s): 347 - 351 , DOI: 10.1109/ISED.2011.37
[94] Mohan, M. ; Anurenjan, P.R. , A new algorithm for data hiding in images using contour let transform, Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE , Page(s): 411 - 415 , DOI: 10.1109/RAICS.2011.6069345
[95] Nugraha, R.M. , Implementation of Direct Sequence Spread Spectrumsteganography on audio data, Electrical Engineering and Informatics (ICEEI), 2011, Page(s): 1 – 6, DOI: 10.1109/ICEEI.2011.6021662
[96] Pramitha, K. ; Suresh, L.P. ; Shunmuganathan, K.L. , Image steganography using mod-4 embedding algorithm based on image contrast, Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 , Page(s): 364 - 369 , DOI: 10.1109/ICSCCN.2011.6024576
[97] Hui-Yu Huang ; Shih-Hsu Chang , A 9/7 wavelet-based lossless data hiding, Computational Intelligence for Multimedia, Signal and Vision Processing (CIMSIVP), 2011, Page(s): 1 – 6, DOI: 10.1109/CIMSIVP.2011.5949236
[98] K. B. S. Kumar, T. Khasim, K. B. Raja, S. Pattnaik and R. K. Chhotaray, "Dual Transform Technique for Robust Steganography", Computational Intelligence and Communication Networks (CICN), **(2011)**, pp. 310 – 314.
[99] G. Chen, C. Min, D. Fu and Q. Ma, "Research on an Steganographic Algorithm Based on ImageEdge", Internet Technology and Applications (iTAP), **(2011)**.
[100] G. Luo and K. P. Subbalakshmi, "Zero Kullback-Liebler Divergence Image Data Hiding, Global Telecommunications Conference (GLOBECOM)", **(2011)**, pp. 1 – 5.
[101] A. A. Al-Ataby and F. M. Al-Naima, "High Capacity Image Steganography Based on Curvelet Transform", Developments in E-systems Engineering (DeSE), **(2011)**, pp. 191 – 196.
[102] T. Meenpal and A. K. Bhattacharjee, "High Capacity Reversible Data Hiding Using IWT", Electronic System Design (ISED), **(2011)**, pp. 352 – 357.
[103] S. Katiyar, K. R. Meka, F. A. Barbhuiya and S. Nandi, "Online Voting System Powered by Biometric Security UsingSteganography", Emerging Applications of Information Technology (EAIT), **(2011)**, pp. 288 – 291.
[104] I. S. Bajwa and R. Riasat, "A new perfect hashing based approach for secure stegnography", Digital Information Management (ICDIM), **(2011)**, pp. 174 – 178.
[105] A. Saha, S. Halder and S. Kollya, "Image steganography using 24-bit bitmap images, Computer and Information Technology (ICCIT)", **(2011)**, pp. 56 – 60.
[106] J. K. Mandal and A. Khamrui, "A Genetic Algorithm based steganography in frequency domain (GASFD)", Communication and Industrial Application (ICCIA), **(2011)**, pp. 1 – 4.
[107] M. J. Khosravi, S. Ghandali, "A secure joint wavelet based steganography and secret sharing method", Information Assurance and Security (IAS), **(2011)**, pp. 222 – 227.

[108] A. Dutta, A. K. Sen, S. Das, S. Agarwal and A. Nath, "New Data Hiding Algorithm in MATLAB Using Encrypted Secret Message", Communication Systems and Network Technologies (CSNT), **(2011)**, pp. 262 – 267.

Authors

Muhammad Khurrum Rahim, He is currently a student of Electrical Engineering BS (EE) in NUCES FAST Islamabad, Pakistan for the session 2013-2017. He has won the competition of English Creative writing in 2007 held in Pano Akil Region, Pakistan by APS&CS. He has one gold and three silver medals in Inter School Mega Competition 2012 and Inter School Mega Competition 2013 in Pano Akil Region, Pakistan by APS&CS. His fields of interest include Robotics, Image Processing, Signal Processing, Circuit theory, Differential and Telecommunication

Aqsa Rashid, She received her MSCS degree in 2015 from Islamia University of Bahawalpur, Pakistan. She attended Islamia University of Bahawalpur, Pakistan for her MCS degree and completed in November, 2012 with a Gold Medal and specialization in Digital image processing and Information security. Her fields of interest include Information security, Robotics, Digital image Processing, Artificial Intelligence, Pattern recognition, Data Mining and Web Designing and Development. Currently she is engaged in real time image processing and computer vision projects.