I. J. Computer Network and Information Security, **2016, 3, 27-33**
Published Online March 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.03.04

Double Layer Image Security System using Encryption and Steganography

Samreen Sekhon Brar
Rayat-Bahra University, Mohali, 140301, India
Email: samreensekhon14@gmail.com

Ajitpal Brar
XNS GLOBAL, Mohali, 160062, India
Email: brarajit18@gmail.com

Abstract—The image security on internet transfers is the concern of the hour as the breaching attacks into the image databases are rising every year. The hackers take advantage of the stolen personal and important images to fulfill their dangerous and unethical intentions. The image data theft can be used to defame a person on the internet by posting the illegal and unacceptable images of that person (internet user). Hence the images transfers have to be secure to ensure the privacy of the user's image data. In this research, a number of image security systems have been studied to evaluate the research gap. Majority of the existing image security systems are not up to date to protect against the latest breaching attacks. So, we have proposed an effective and robust image security framework particularly designed for the images. The proposed has been designed and implemented using MATLAB. In this research, a hybrid image security framework has been proposed to overcome the problem stated earlier, which will be implemented by combining various techniques together to achieve the image security goal. The techniques included in the combination would beimage compression, cryptography and steganography. DWT compression has been used, because it is a stronger compression algorithm. The steganographed image would be compressed to reduce its size. Blowfish encryption algorithm would be used for the encryption purposes. It offers maximum throughput (faster) and also energy efficient. Compressed image would be encrypted to enhance the image security. Real image will be hidden into another image. A cluster based steganographic technique will be used. Real image and face image would be analyzed, and the real image would be embedded in those areas of face image, where color schemes of the real image and face image would be most similar. Kmeans or Hierarchical clustering would be used as a clustering technique. An all new comparative analysis technique would be applied to make the comparison between real image and base image on the basis of color patterns.

Index Terms—Image Security, Image compression, Image steganography, Image encryption, image transfers.

I. Introduction

Digital multimedia is data can be delivered over the computer networks, which is prone to the security breaches. The countries launch the space missions to get the information about the existing elements in the space. [5] The countries don't want the information to get leaked. [11] So there must be security mechanism which can ensure the security of inter-space transmissions. [3, 7] Under this research we are proposing secure mechanism to secure the images in the inter-space communications. As we know that, digital data can be copied without any loss in quality and content. [14] This poses a big problem for the protection of intellectual property rights of the countries and space agencies own that data. Hybrid image security is a solution to the problem. It includes a combination of steganography, cryptography and compression. [1]

Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. [13] Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. [12] Steganography is not as robust to attacks since the embedded data is vulnerable to destruction. Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. [11, 15] Only those who possess a secret key can decipher (or decrypt) the message into plain text. [2, 4] Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable. [6] In computer science and information theory, data compression, source coding, or bit-rate reduction involves encoding information using fewer bits than the original representation. [8] Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying unnecessary information and removing it. [10] The process of reducing the size of a data file is popularly referred to as data compression, although its formal name is source coding (coding done at the source of the data before it is stored or transmitted). [9]

With the fast growing network, many people utilize the various applications to transfer digital image data. Most of people share their personal images with other users using the social application. Hacking attacks on these applications can cause great losses to the user security which can lower the number of active users and so the business popularity. [11] Now-a-days users access these applications from their portable devices (smart phone, tablet, etc.). To prevent the hacking attacks on those web or mobile application architectures, there is various data security mechanism for image, video or text data. [14] These existing security mechanisms are either using encryption or steganography, or their combinations. There is various securable and perfect system of image encryption that can be well protected from unauthorized access [1]. When it comes to the image transfers over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. To achieve the goal of image security, a number of image security and image processing algorithms are in use individually or in a combination to provide the effective image security. But these existing image security mechanisms fail to provide the best image security and sometimes proved to be breakable or hack-able. Image compression is an additional function, which can be applied on the image to lower their memory size. The known and popular algorithms used for the data compression are DFT, DCT, DWT, etc. [1].

Image transfers over internet or intranet are prone to hacking. The image transferred over internet or intranet can be hacked by hackers using some attacks: [2].

- Passive attacks: A passive attack attempts to learn or make use of information from the system but does not affect system resources. It is of two types: Release of message content, Traffic analysis. [11-13].
- Active attacks: Active attacks involve some modification of the data stream or the creation of a false stream. And subdivided into masquerade, replay, and modification of messages and denial of service. [1-2. 6, 8, 9-10].

End to end authentication can be also used to keep image transfer integrity intact, but end to end authentication is not possible in case of many image transfers, because many server based internet services like Facebook, Whatsapp, etc. does not let a user to save the content in secure formats, and does not allow the end-to-end authentication based protocols [2].

II. Literature Review

Eman A. Al-Hilo, Rusul Zehwar [2014]: In this paper, the fractal pressure system proposed by Jacquin is examined for 24 bits/pixel shading picture. The information of the shading segment (R,G,B) are changed to (YIQ) shading space, to exploit the current unearthly connection to acquire pressure. Additionally the low spatial determination of the human vision frameworks to the chromatic parts (I, Q) was used to build the pressure proportion without making huge subjective bending. The test outcomes demonstrate that PSNR (31.05) dB with CR (8.73) and encoding time (57.55) sec for Lena picture (256x256) pixel. Xiangui Kang, Jiwu Huang [2003]: In this paper, the water checking extraction has been shown for JPEG pressure. In watermark extraction, creators at first recognize the layout in a perhaps tainted watermarked picture to acquire the parameters of relative change and proselyte the picture back to its unique shape. At that point they have performed interpretation enlistment by utilizing the preparation succession installed as a part of the DWT space lastly extricate the useful watermark. Trial works have exhibited that the watermark produced by the proposed calculation is more vigorous than other watermarking calculations reported in the writing. Particularly it is hearty against all relative change related testing capacities in StirMark 3.1 and JPEG pressure with quality variable as low as 10 at the same time. While the methodology is introduced for dim level pictures, it can likewise be connected to shading pictures and feature groupings. Creighton T. R. Hager worked on the Performance and Energy Efficiency of Block Ciphers in Personal Digital Assistants [3].The author has performed a comparative analysis of various encryption algorithms on various kinds of data. This research has proved that blowfish outperforms all other encryption algorithms. Blowfish is the best, unbreakable and fast encryption algorithm than others. Gary C.Kessler has written an Overview of Cryptography: Cryptographic [3]. This is an old published paper on cryptography by Gary C. Kessler, and since then it was continuously updated till date. It was last updated in 2014. The author suggested the great source for the cryptography algorithms again. It is very important to understand the encryption algorithm structure before putting it in the use. Navita Agarwal et al. have develope Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography [1]. The authors have conducted a similar research, where they have applied compression, encryption and steganography on the digital image data. Pixel shuffling based symmetric encryption algorithm, DCT for compression, WinRAR to Image steganography are used to achieve the proposed model in this paper.

Gary C.Kessler has also written an overview of steganography for the computer forensics examiner [9]. This is an online article and it is continuously updated. This link is the best source for the information and study about the various encryption algorithms, their working flow, algorithmic structure, etc. This link proved to be the major source behind my encryption algorithm studies. Chanu Y. J, have given a Survey on Image Steganography and Steganalysis [6]. In this paper, the authorhas conducted a detailed survey on various steganography techniques. From this paper it is easy to understand and compare the steganography techniques.

This paper is the major source behind my study on steganography. Chamkour Singh *et al.* have developed cluster based Image Steganography using Pattern Matching"[7]. A novel steganography technique is proposed in this paper, which perform color based analysis on the image by using color clustering technique to hide the image data effectively into another image. This method is more secure than all other image steganography methods because it makes it difficult to detect the hidden image in the masking image.

III. Experimental Design

Our first goal in this project is the image compression. Various compression schemes have been studied under the first objective. The major compression schemes evaluated under the preliminary study for this research are DFT (Discrete Fourier Transformation), DCT (Discrete Cosine Transformation) and DWT (Discrete Wavelet Transformation) because of their popularity and effectiveness. [10, 11] For images, the JPEG images are taken into account as it preferred DWT over DCT or DFT. [12, 13] In DFT, execution time is lower and it provides lower compression as compare to the other techniques. In DCT is simple compression algorithm, because computation count in this algorithm is limited, hence provides lower compression ratio. DWT on the other hand, is complex and computation count is very high and it provides higher compression ratio as compared to later two and also proven to be more effective. In wavelet transform system the entire image is transformed and compressed as a single data object rather than block by block as in a DCT based compression system. It can provide better image quality than DCT, especially on higher compression ratio. [10] After preliminary study of literature based on these compression techniques we evaluated that DWT with HAAR Wavelet is the best performer among all other compression techniques available in our selection in terms of compression ratio and elapsed time. Finally, the decision is made to use DWT for its effectiveness and robustness over DCT and DFT. [10, 11]

Algorithm 1: Compression Method

```
1. The image is broken in smaller parts, say 8x8 pixels
2. Working from left to right, top to bottom, the DWT is applied to each block
3. Each block is compressed through quantization
4. The array of compressed blocks that constitute the image is stored in a drastically reduced amount of space.
5. When desired, the image is reconstructed through decompression, a process that uses the inverse discrete wavelet transform (iDWT).
```

To perform the encryption in the second object, blowfish encryption algorithm is used to hide the image details of hidden object. [1,3-4,8] A significant number of research papers on the performance evaluation and work flow of encryption algorithms has been studies under the literature survey part. The AES and Blowfish algorithms were selected in the final short listing of encryption algorithms, because these two provide the best encryption security. [4, 8] Out of the two shortlisted ones, the conclusion was obtained that the blowfish encryption algorithm is considered the fastest one among the all other options. [4] Blowfish encryption algorithm is designed in a customized way to work with images in MATLAB environment. The algorithm code is designed to perform various rounds of encryption. The encryption algorithm is used here to hide the image details and to create a new image with dizzy image details. The image details are made hidden in chaotic way to create a new image with less number of details. The image is not made completely unreadable because it provokes the hacker to crack into the encryption, whereas a low resolution less detail encryption can be easily mistaken as a bad image. [3, 8]. The decryption process is the reverse process, which is used to obtain the original image by using the reverse engineering of the cryptographic process on the receiver's end. [3] For the decryption, user has to enter the same key as it was entered on the sender's side while encrypting the image. The decryption process returns the full resolution original image from the encrypted image once the process is complete. [8]

Algorithm 2: Blowfish encryption

```
Blowfish has 16 rounds.
1. Input block size is 64-bit, denoted as x
2. Break x into two elements of 32-bit each, denoted xL, xR
3. Then, Start for loop with syntax, for i = 1 to 16:
4. $xL = (xL * XOR * Pi)$        (1)
5. $xR = F(xL) * XOR * xR)$        (2)
6. Then Swap the xL and xR data matrices
7. When the 16th round will be finished, re-swap xL and xR to undo the swap on step 6.
8. Then, xR will be created by using P17 and P18 instead of Pi in (1)
9. In the final step, again combine the xL & xR to return the cipher data.
```

To perform the steganography in the third objective, which is used to embed image(secret object) into image (cover object), A number of papers have studied for the selection of best steganography technique for the development of our security model.[5, 6, 7, 9, 12, 13] Steganography is a security mechanism which is used to hide the message into another object which may be a text, image, audio, video etc. 2-D discrete wavelet transform has been used to perform the decomposition of the image matrix up to two level decomposition. DB1 or HAAR wavelet is used for the decomposition to compute the 2-D DWT decomposition for steganography.[5, 6] This decomposition will produce four decomposed matrices which include CA (Absolute Coefficient) and CD (Detailed Coefficient) in the first level and again applying filtering on these coefficients will produce CH (Horizontal Detailed Coefficient), CV (Vertical Detailed Coefficient) in the second level.[Coutesy: Wikipedia]

After applying the compression on the hidden object image, the very next step is to hide it inside the decomposed cover object. [1, 5-7] The hidden object is hid inside the most similar decomposition matrix of cover object. The similarity between the decomposed matrices and hidden object will be found by using the color based image analysis. [7] To hide the hidden object, the two matrices would be combined using the ordinary matrix calculations. The decomposition matrices would be recomposed to form the stego object image and an index value is embedded inside the stego object to identity the specific decomposition matrix in which the hidden object is embedded. [5-6]. For steganalysis or image extraction, the stego object undergoes the decomposition using the HAAR wavelet. [5] The program reads the index to identify the decomposition matrix where the hidden object was embedded. The specific decomposition matrix undergoes the extraction process using the reverse matrix calculation to obtain the secret image hidden inside it. [1, 6-7]

Algorithm 3: Steganography Method

A. At Sender side:

1) *Input Image*: Select a color image to be used as a cover media.
2) *Pattern Matching*: Scan image according to basic colors by using pattern matching.
3) *Clustering*: Create cluster (using pattern matching) based on color feature.
4) *Selection of Cluster*: Select cluster in which the secret data is to be hidden.
5) *Apply Steganography*: Hide data in the color image.
6) *Send Image*: Send the stego-image over the channel.

B. At Receiver side:

1) *Input Stego-Image*: Take the stego-image as input.
2) *Pattern Matching*: Scan image by using pattern matching.
3) *Clustering*: Create cluster according to color.
4) *Identify Cluster*: Identify the cluster in which information is hidden.
5) *Extraction*: Extract the hidden data.

The fourth objective is yet partially achieved by implementing the code for compression and steganography in MATLAB using normal coding in Matlab and Image Processing Tool Box. The compression module is completed by using 2-D HAAR wavelet for decomposition of image matrix using Haar wavelet based low pass and high pass filter and results in Approximation Coefficient Matrix and Detailed Coefficient Matrix. Then built-in Matlab function for calculation of threshold using Birge-Massart Algorithm based on 2-D wavelet. This capacity returns level-subordinate edges THR and quantities of coefficients to be kept NKEEP, for de-noising or pressure. THR is gotten utilizing a wavelet coefficients determination tenet in view of the Birge-Massart technique. [14] In next step, the threshold value will been used to perform the compression on the image matrix. This step returns a de-noised or compressed version of 2-D image matrix from input image matrix obtained by wavelet packets coefficients thresholding, again based on HAAR wavelet.

IV. Result Analysis

This work is carried out in MATLAB version 2011a on Laptop (*Dell*): Intel (R) Core (TM) i3-2430M CUP @ 2.40 GHz Processor, 64-bit Operating System and 4.00 GB RAM. To evaluate the performance of the established color FIC system by RGB model, the proposed system has been tested using image dataset as test images. These tests explore the effect of the following coding parameters on the compression performance parameters of the established system: This set of tests was conducted to study the effect of MinScale, and MaxScale of quality on the compression performance parameters of the reconstructed image. In these tests the value of compression parameters are set in table (1). The effects of this test shows in table (1 and 2). Figure (1, 2, 3 and 4) shows the results of this test graphically.

Table 1. The Comparison of Images of Various Categories in the Image Dataset

Image Group in Dataset	Images	PSNR	CR	ET	MSE
	0-7	48.58	42.58	Com: 0.420 Cryp: 0.87 Stego: 6.79 Total: 8.093	1.23
	8-19	53.76	43.49	Com:0.398 Cryp: 0.86 Stego: 6.80 Total: 8.070	0.54
	20-29	47.61	43.56	Com: 0.40 Cryp: 0.86 Stego: 6.80 Total: 8.069	1.82
	30-39	49.01	43.46	Comp: 0.41 Cryp: 0.86 Stego: 6.80 Total: 8.083	0.88
	40-49	49.14	73.22	Comp: 0.408 Cryp: 0.872 Stego: 6.854 Total: 8.135	1.98
	50-52	45.68	42.16	Comp: 1.168 Cryp: 0.883 Stego: 6.857 Total: 8.909	2.10

The above table is representing the results of the proposed algorithm on the selected image dataset. The image dataset is carrying total 52 images in 6 major categories. The first category of images belongs to the noisy images clicked by low resolution cameras. These images are mostly prone to the processing noises and their image quality gets more degradation that any other type of images during the matrix transform processing like compression, encryption, steganography, etc. The second category belongs to the images of nature, especially beaches. These images have higher and dense color range within less basic colors. For example, the image carrying the scene of ocean is having multiple color densities of blue color in them, which are more prone to loss of the details during the processing. The third types of the images are green infrastructure, which are carrying less number of colors than the other images. These images are less prone to the system of transmission noises. The fourth type of images belongs to the urban transportation category. These images are representing on dominant color over the other, hence the effects of processing and transmission noises effects on one color can be studied. The fifth type of images belongs to the digital image category. The digital images fall in the noisy image category. The human cannot determine the noise in these images. But, sometimes, the noise degrades the image quality at a large. The sixth type of images is grayscale image. These images carries lower color details and prone to processing and transmission noises.

Table 2. Comparison of Existing Technique with Existing Technique

Image Group in Dataset	Data Set Index	PSNR		Compression Ratio (CR)		MSE		Elapsed Time (ET)	
		Proposed	Existing	Proposed	Existing	Proposed	Existing	Proposed	Existing
	0-7	48.58	30.65	42.58	5.237552	0.420	1.90	1.23	3.54
	8-19	53.76	29.42	43.49	14.71	0.398	0.69	0.54	1.80
	20-29	47.61	14.94	43.56	11.96	0.40	1.45	1.82	3.12
	30-39	49.01	26.37	43.46	9.79	0.41	0.504	0.88	2.10
	40-49	49.14	37.48	73.22	12.37	0.408	0.819	1.98	4.04
	50-52	45.68	35.13	42.16	21.04	1.168	1.56	2.10	3.68

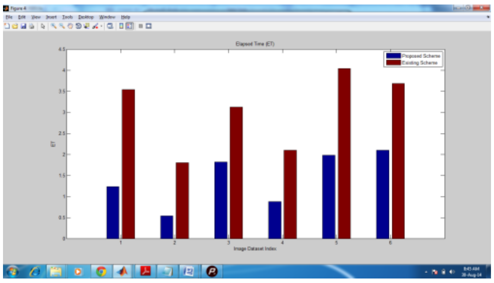

Fig.1. Elapsed Time between Proposed and Existing System

Elapsed time is the total time taken by system to execute its operations for compression mechanism on the selected data. The above graph has clearly shown that proposed algorithm has done way better than the existing algorithm. The elapsed time of the proposed algorithm is lower for all image categories in the dataset.

PSNR represents the quality of the image by comparing images of before and after processing on the selected image data. The above graph has clearly shown that proposed algorithm has done way better than the existing algorithm in the terms of PSNR. The PSNR value is higher in the case of proposed algorithm than the existing algorithm for all image categories in the dataset, which shows that proposed algorithm creates clearer image at the end of the processing.

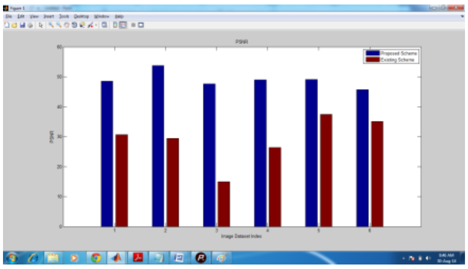

Fig.2. PSNR Comparison between Proposed and Existing System

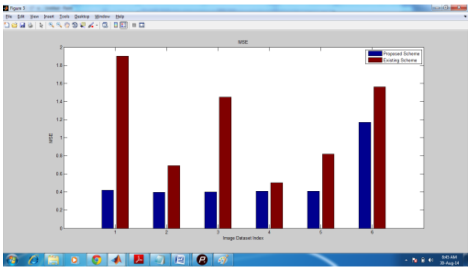

Fig.3. MSE Comparison between Proposed and Existing

Mean squared error is calculated by calculating the error bits over all bits, which represents the total error in the received data when it is compared to the data sent at the other end or data before and after processing. MSE value should be less to represent the less damage to the quality of the image. In the above graph, the MSE value for proposed system is lower as compared to the existing system on different image categories in the image dataset.

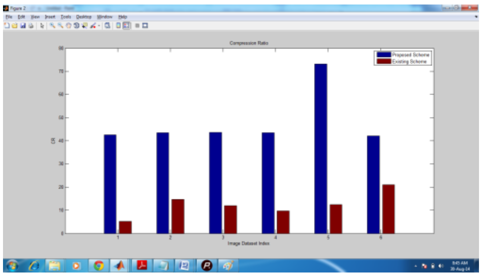

Fig.4. Compression Ratio

Compression Ratio represents the reduction in the size of the image after the compression process. Higher is the compression ratio; lower is the transmission effort and disk space consumption. In the case of proposed model, the compression is recorded way higher than the existing model.

V. Conclusion

The proposed scheme is developed to ensure the more image security during transmission by facilitating the quick image transfers. Also the processing image security mechanism had to be effective in the terms of elapsed time. Elapsed time is the term used for time taken for the image processing during various transform operations. The image quality has been measured using various performance parameters like Peak signal to noise ratio (PSNR) and mean squared error (MSE). The proposed scheme consisted of three components: compression, encryption and steganography. For the compression, the discrete wavelet transform is modified for robust image compression, whereas the blowfish algorithm has been selected for the image encryption. The image encryption hides the image details by performing mathematical computation on image data. The steganography is the process of hiding one image into another image to fool the hackers and to deliver the secret data without any visual data transmission details. The proposed algorithm has been designed to ensure the image security during the transmission over the image sharing enabled social media applications. These applications usually do not have strong security mechanisms to protect the user data. The proposed algorithm is designed to fill that certain gap of stronger security mechanism for image sharing based social media applications. The results of the proposed algorithm have shown that the proposed algorithm have performed more stronger and lossless compression on the images in comparison with the existing compression system. The overall system performance has been evaluated with four performance parameters: Peak signal to noise ratio (PSNR), mean squared error (MSE), Elapsed time (ET) and Compression Ratio (CR). The overall system performance has shown that the new system is robust, quick and effective for the image security. The proposed system has been tested on a classified image dataset. The image dataset is shortlisted to five six categories. The results on all of the six categories have proved the proposed system better than the existing system.

VI. Future Work

In the future, the proposed security mechanism can be improved to generate better and quick results. Also, other forms of compression, steganography or compression can be tried with the proposed system to take the advantage on different type of datasets of images or other type of digital media. The proposed algorithm can be implemented on the live system to obtain its performance in the real time on the application server in the future.

References

[1] NavitaAgarwal, Himanshu Sharma "An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography", IJCSMC, vol. 2 issue 5, pp. 376-385, May 2013.

[2] Mohammadi S., Abbasimehr H., "A high level security mechanism for internet polls", ICSPS, vol. 3, pp. 101-105, IEEE, 2010.

[3] Gary C.Kessler, "An Overview of Cryptography: Cryptographic", HLAN, ver. 1, 1999-2014.

[4] Milind Mathur, Ayush Kesarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES", NCNHIT vol. 1 143-148, 2013.

[5] Ashwin S., "Novel and secure encoding and hiding techniques using image steganography: A survey", ICETEEEM, vol. 1, pp. 171-177, IEEE, 2012.

[6] Chanu Y. J, "A short survey on image steganography and steganalysis techniques", NCETAS, vol. 1, pp. 52-55, IEEE, 2012.

[7] Chamkour Singh, Gauravdeep, “Cluster based Image Steganography using Pattern Matching”, IJAIR, vol. 2, issue 5, 2013.

[8] Verma O.P., Agarwal R., Dafouti D., “Performance analysis of data encryption algorithms”, ICECT, vol. 5, pp. 399-403, IEEE, 2011.

[9] Gary C.Kessler, “An overview of steganography for the computer forensics examinier”, vol. 6, no. 3, Forensic science communications, 2011.

[10] Xiangui Kang, Jiwu Huang, “A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression”, ITCSVT, vol. 13, issue 8, pp. 776-786, IEEE, 2003.

[11] Sonja Grgic, Mislav Grgic, “Performance Analysis of Image Compression Using Wavelets”, ITIE, vol. 48, issue 3, pp. 682-695, IEEE, 2001.

[12] Domenico Bloisi and Luca Iocchi, “IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY”, *Sapienza University of Rome, Italy, 2002.*

[13] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." *ISSA*. 2005.

[14] Jalal Karam, “A New Approach in Wavelet Based Speech Compression”, Mathematical Methods, Computational Techniques, Non-Linear Systems, Intelligent Systems, pp. 228-233, 2008.

[15] IngYannSoon, FengZhou, ZhenLi, HaijunLei, Baiying Lei, A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition, Signal Processing, vol. 92, pp. 1985-2001, Science Direct, 2012.

Authors’ Profiles

Samreen Sekhon Brar, born in 1986, MCA and assistant professor in Rayat Bahra University. Her main research interest are image processing and data mining.

Ajitpal Brar, born in 1984, independent research and director at XNS GLOBAL. His main research areas are image processing and information security.

How to cite this paper: Samreen Sekhon Brar, Ajitpal Brar,"Double Layer Image Security System using Encryption and Steganography", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.3, pp.27-33, 2016.DOI: 10.5815/ijcnis.2016.03.04