World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.218

SECURE TRANSACTION USING VISUAL CRYPTOGRAPHY AND STEGANOGRAPHY

Shweta Sisodiya* and Kiran Dange

Electronics and Communication Engineering Department, Usha Mittal Institute of Technology, SNDT Women's University, Santacruz West, Mumbai.

Article Received on 22/02/2018 **Article Revised on 15/03/2018** **Article Accepted on 05/04/2018**

***Corresponding Author**
Shweta Sisodiya
Electronics and Communication Engineering Department, Usha Mittal Institute of Technology, SNDT Women's University, Santacruz West, Mumbai.

ABSTRACT

It is not safe to rely on internet to store all the information because of tremendous realization and growth in the field of internet technology and hacking. For personal privacy protection, it's needed to secure data while transmission through electronic media. Image encryption is one of the innovative are a in this era of Internet technology. The algorithm mainly deals with Image Processing, Visual Cryptography and Steganography. In this paper, any image from the applicant is processed in such a way that it is pre-processed and encrypted first using standard AES algorithm. Pixels of encrypted image are modified by Chaotic Genetic Algorithm. This modified image is embedded in Cover image using Steganography. Decomposition of this image is done using Discrete Wavelet Transform. One approximate share of output image is given to the applicant and all other shares are preserved in the database. The applicant need to provide his share during every transaction and those shares are over lapped with the already existing shares in the database and a check for authentication is done by using correlation technique. If a higher correlation co-efficient is achieved, then the authentication is succeeded. Also, value of MSE is lower so the Error.

KEYWORDS: Visual cryptography, Steganography, Chaotic Genetic algorithm, AES encryption.

INTRODUCTION

The Internet provides a wealth of information and services. Many activities in our daily lives now rely on the Internet, including various forms of communication, shopping, financial services, entertainment and many others. The growth in the use of the Internet, however, also presents certain risks. Just think about all the information you send over the Internet, such as personal messages, bank account information, photographs, etc.

Information technology security becomes more important when operating a business online. It's critical to take the steps necessary to protect an online business against hackers who could steal vital information, or viruses which could bring your computer system to knees.
There are many criminals on the web creating viruses, hacking, trying to steal identities, and more. For the most part, the Internet is indeed private and secure, but there are a number of serious security risks.

Proposed method uses different image processing methods for enhancing secure online transaction. AES, chaotic genetic algorithm steganography are used for visual cryptography.

PROBLEM DEFINITION

It is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. The question is how to handle applications that require a high level of security, such as core banking and internet banking. In a core banking system, there is a chance of encountering forged signature for transaction. And in the net banking system, the password of customer may be hacked and misused.

Thus, security is still a challenge in these applications. In today's world, the major issue in banking sector is authenticity of customer to bank and vice- versa. Visual cryptography is one of the most prominent ways to provide authentication because it allows hiding the data and its secure transmission on open communication channel, giving secure bank transaction. The problems with the existing methods are as follows:
Rotation attacks, Scaling Attacks, Cropping attack, loss of compression.

PROPOSED ALGORITHM

The proposed scheme deals with different Encryption methods of Image processing for securing secret data. Steps in Encryption and Decryption are explained below. Fig.1 shows the Block diagram of proposed scheme.

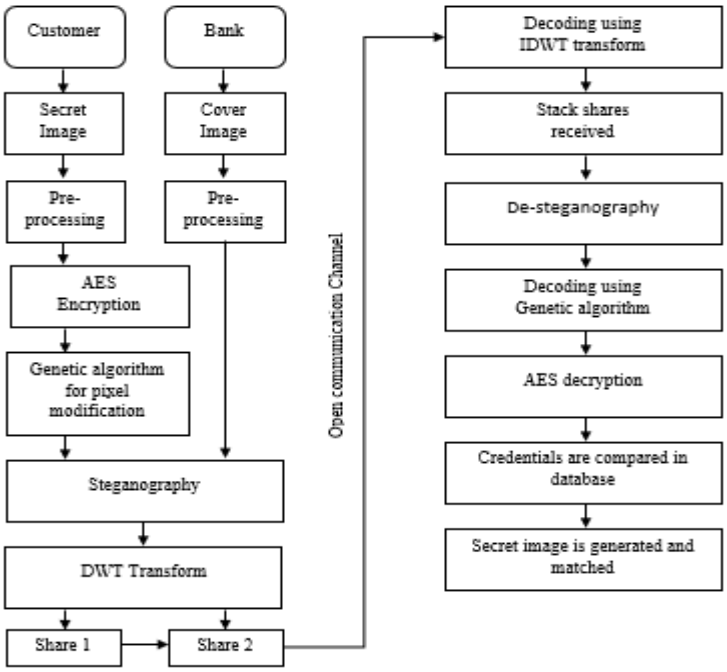

Figure 1: Block diagram of proposed scheme.

2.1. Input: Take Secret image and Cover image as Input image. Cover image is not changeable without permission of bank. Secret image is provided by Customer.

2.2. Preprocessing: Image denoising algorithms attempt to remove noise from the image. Non-local means filtering takes a mean of all pixels in the image, weighted by how similar these pixels are to the target pixel. This results in much greater post-filtering clarity, and less loss of detail in the image compared with local mean algorithms.[12]

2.3. Advance Encryption standard for Encryption

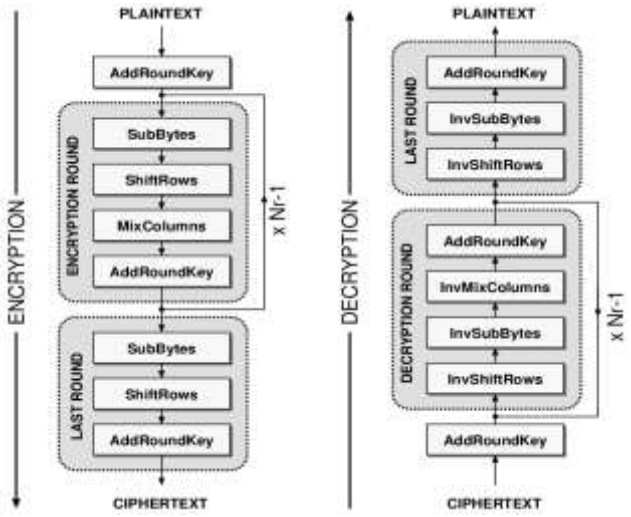

Figure 2: Algorithm of Advance Encryption standard for Encryption.

Cryptography is necessary when communicating over any unreliable medium which includes any network like internet. A standard 128-bit or 256-bit AES Encryption and Decryption method is used for converting Secret image into a code, especially to prevent unauthorized access.[2]

AES is a symmetric encryption algorithm processing data in block of 128/192/256 bits. The only secret necessary to keep for security is the key.

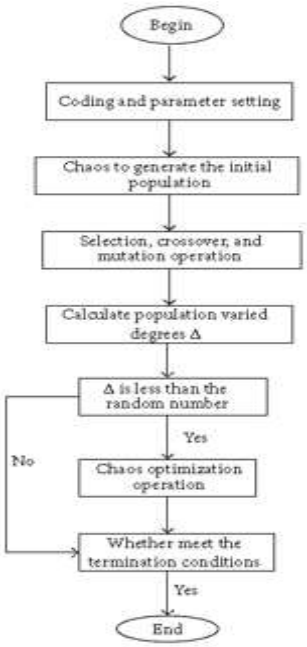

Figure 3: Chaotic Genetic Algorithm.

Figure2 shows Algorithm of Advance encryption standard for Encryption. For the AES algorithm, the length of the Cipher Key, K, is 128, 192 or 256 bits. The key length is represented by Nk = 4, 6, or 8 which reflects the number of columns in the Cipher Key. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by Nr, where Nr = 10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8.[2]

2.4. Chaotic Genetic Algorithm

Chaos is a bounded dynamic behavior that it occurs in deterministic nonlinear system. Although, it appears to be stochastic, it occurs in a deterministic nonlinear system under deterministic conditions.[4] It is highly sensitive to changes of initial condition than a small change to initial condition can lead to a big change in the behavior of the system. Chaos theory is typically described as the so-called ‘butterfly effect’ detailed by Lorenz.[5]

There are three main properties of the chaotic map, i.e.

- Ergodicity.
- Randomness.
- Sensitivity to initial condition.

Making it very suitable for digital image encryption, forming a kind of chaotic image encryption algorithm. Figure 3 shows Chaotic genetic algorithm for encryption.

Genetic algorithm is different from traditional search algorithm; The genetic algorithm steps are as follows: (1) Randomly generate initial population. (2) Go through fitness function to evaluate the chromosomes. (3) Select chromosomes according to the fitness level and form a new population. (4) Go through crossover and mutation operation which produces new chromosomes that offspring. (5) Repeat steps (2) - (4), until getting the scheduled evolution algebra.

It generates a new species to reach the purpose of searching the global optimal solution. Its evolutionary computation is through the competition mechanism constantly updating population process.

Crossover operation is the main genetic algorithm; the performance of genetic algorithm depends largely on the performance of its adopted crossover operation. Crossover operation operates the two chromosomes at the same time, combining the two features to produce new offspring. Variation is a basic operation; it spontaneously generates random variation on chromosome. Variation can offer gene which is not contained in the initial population or find missing gene in the selection process, providing new content for population.[6]

Advantages of Genetic Algorithm

It is faster and more efficient as compared to the traditional methods.

Optimizes both continuous and discrete functions and also multi-objective problems.

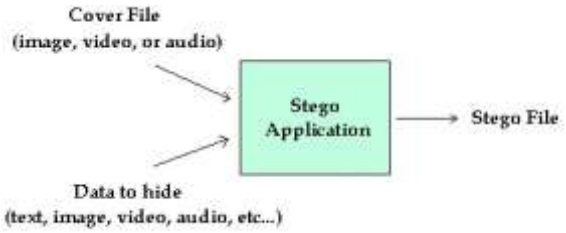

Figure 4: Steganography.

2.5. Steganography: Steganography is a technique of hiding information in digital media. The goal of Steganography is to avoid drawing suspicion to the existence of a hidden message. It is the art of invisible communication by concealing information inside other information. In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. A Steganography system as shown in figure 4 consists of three elements: cover image (which hides the secret message), the secret message and the stegano-image (which is the cover object with message embedded inside it).[7]

The LSB based image steganography is used to embed the secret in the least significant bits of pixel values of the cover image.

Encryption process: Read the secret and cover image and convert them into gray scale images, then check the size of the secret image with that of the cover image such that size of the secret image should be less than cover image. Encode the secret image into binary using bit gate command and divide it into RGB parts then substitute MSB bits of secret image into LSB bits of cover image.

3.5. Discrete wavelet transform: Wavelet transform decomposes a signal into a set of basis functions. The DWT decomposes a digital signal into different sub bands so that the lower frequency sub bands have finer frequency resolution and coarser time resolution compared to the higher frequency sub bands. Wavelet functions are spatially localized.

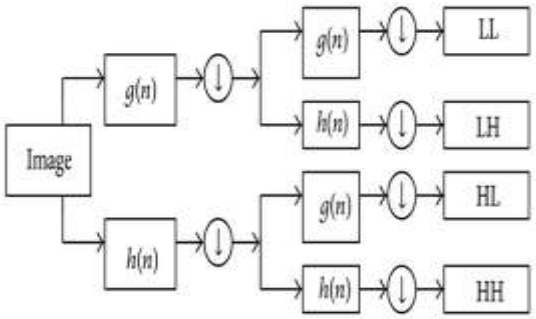

Figure 5: Discrete wavelet transform.

As shown in figure 5, First, we apply a one-level, one-dimensional DWT along the rows of the image. Second, we apply a one-level, one-dimensional DWT along the columns of the transformed image from the first step. As depicted in Figure, the result of these two sets of operations is a transformed image with four distinct bands: (1) LL, (2) LH, (3) HL and (4)

HH. Here, L stands for low-pass filtering, and H stands for high-pass filtering. The LL band corresponds roughly to a down-sampled (by a factor of two) version of the original image. The LH band tends to preserve localized horizontal features, while the HL band tends to preserve localized vertical features in the original image. Finally, the HH band tends to isolate localized high-frequency point features in the image.[13]

RESULTS AND DISCUSSION

To test the proposed, scheme a software application is written in MATLAB2015R. GUI is made in order to carry out the test results, a number of experiments have been carried out by varying the image size. It gives original secret image. Results are shown below:

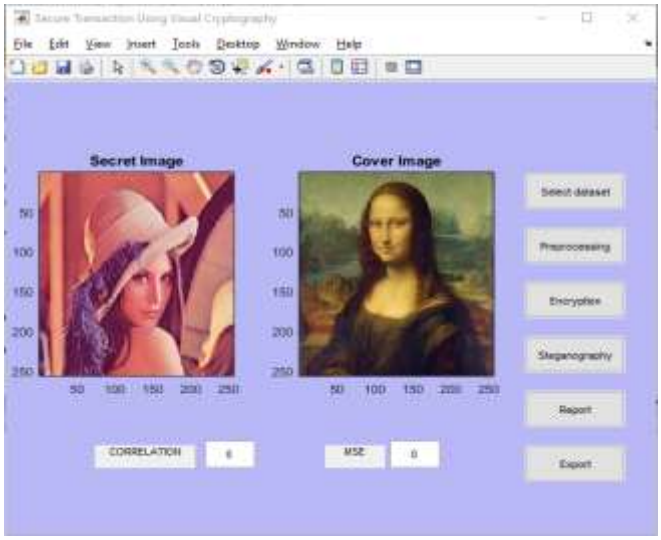

Figure 6: Input Secret image and Cover Image.

Input image

Secret image i.e. Test image Lena is taken as input image. Cover image is Lisa image shown in figure 6.

Preprocessing is done to get clear picture using non-linear means filter.

Figure 7: Steganographed image.

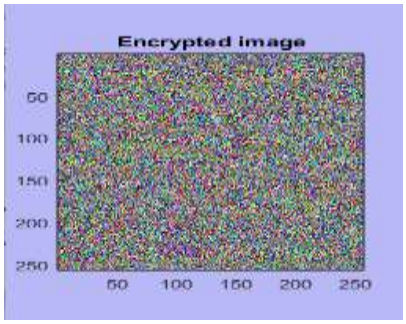

Figure 8: Encrypted image.

Encryption: After application of AES encryption and Chaotic genetic algorithm we get encrypted image as shown in figure 7.

Steganography

Steganography is done to embed encrypted image in cover image. Figure 8 shows output image after steganography.

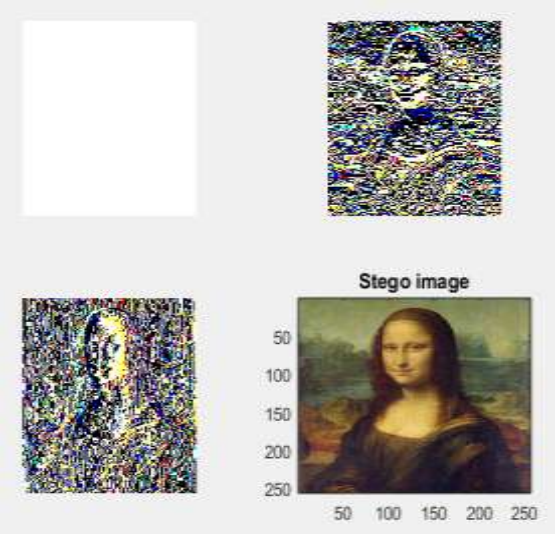

Figure 9: Decomposed Steganographed image.

Discrete Wavelet transform

After DWT is applied we get Decomposed Steganographed image as shown in figure 9. DWT processing output gives four shares which are:

1) Approximate share
2) Horizontal share
3) Vertical share
4) Diagonal share.

Result and Analysis are generated randomly with size up to maximum hiding capacity. Table 1 shows the Value of Correlation and MSE with respect to different image size. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two-error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

To compute PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively.

To ensure the quality, a parameter is developed to compute the quality of the image this parameter is called PSNR and defined as follows:

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})$$

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

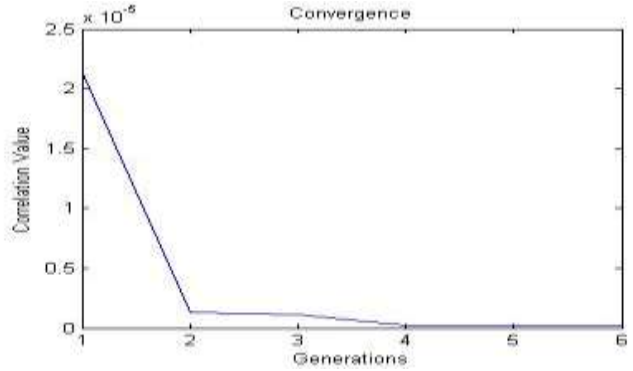

Figure 10: Graph of Correlation value with respect to generation which is used for encryption by using Genetic Algorithm.

The correlation coefficient of two random variables is a measure of their linear dependence. If each variable has N scalar observations, then the Pearson correlation coefficient is defined as

$$\rho\,(A, B) = \text{cov}\,(A, B)/\sigma A.\sigma B$$

where σA and σB are standard deviation of A and B respectively and cov (A, B) is covariance of A and B.

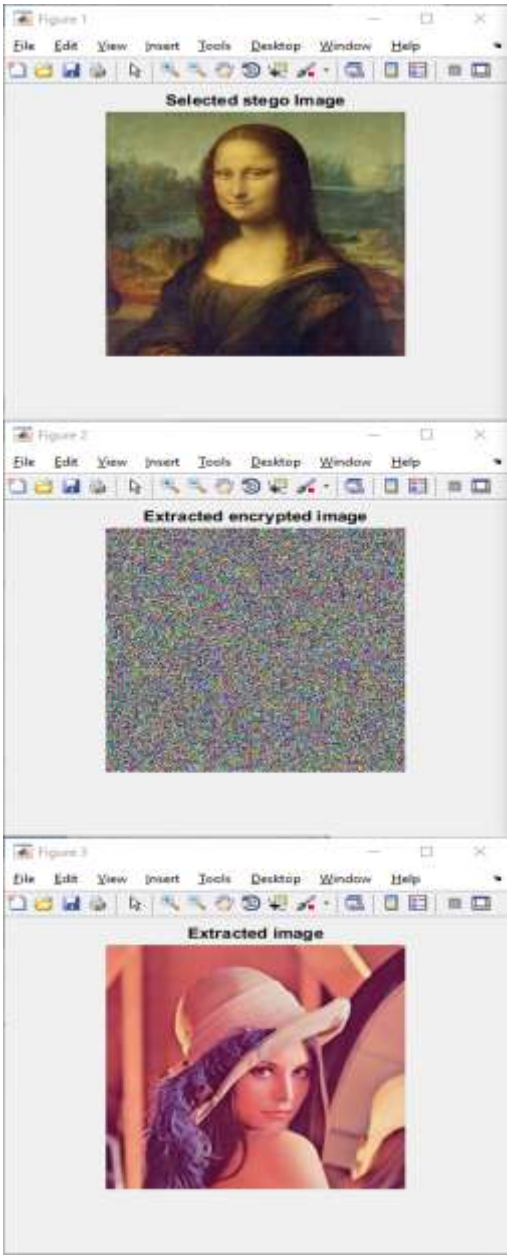

Figure 11: Image at Receiver end, after application of Stegnographed image and the key.

Communication channel is used to send these shares to the Decryption side and Reverse process is applied to get original Secret image. The process is shown below:

1) Take share of stegnographed image from database
2) Take cover image
3) Take key.

After processing at Decryption side, we will get images and original Secret image as shown in Figure 11. If it is the same image that we had applied then the we can say it is from authenticated server and Client.

Histogram

An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

Figure 12 shows the image histogram of Encrypted image and extracted image.
Figure 13 shows the image histogram of Secret and Extracted image.

Image histograms can be useful tools for thresholding.

Figure 12: Histogram of Encrypted image and extracted image.

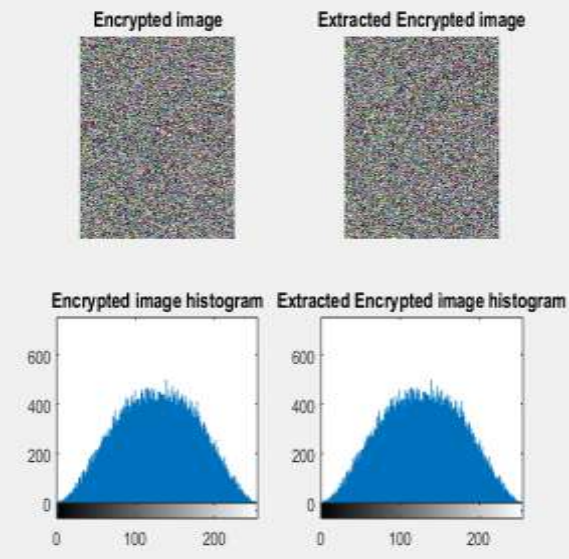

Figure 13: Histogram of Secret and Extracted image.

Table 1: Value of Correlation and MSE with respect to different image size.

Image size(JPEG)	Correlation between Secret image and Cover image	MSE
128 by 128	$8.194\ e^{-5}$	0.1584
225 by 225	0.00012	0.16921
250 by 250	0.00276	0.16939
300 by 300	0.000432	0.147
400 by 400	$5.727\ e^{-6}$	0.166
500 by 500	0.000131	0.1941

CONCLUSIONS

Many secure and confidential data items like Bank passwords are sent over the internet. While using secret documents (images, text etc.) for sending over the network, the security is the main concern. With the help of above proposed system visual information can be securely sent over the internet.

Advantages of our proposed scheme

1. It provides complete Security for the secret images or documents.
2. It is robust method against the loss of compression and distortion and many Geometrical or Scaling attacks as well as rotation attacks providing much security to the secret data that is shared in day to day life.
3. Better noise immunity and better correlation coefficient.

We can implement this type of system in various fields like Bank, Military, Defense, and other places where the confidentiality of the data is must.

ACKNOWLEDGMENTS

I would like to thank my Project guide Ms. Kiran Dange for supporting me in successful completion of this project.

REFERENCES

1. Karishma Patel, Prof. D. R. Kasat, Dr. Sanjeev Jain, “Secure Transaction Using Visual Cryptography”, ISSN(Print): 2454-406X, (Online): 2454-4078, 2015; 1(2).
2. J. Nechvatal, “Report on the Development of the Advanced Encryption Standard (AES)”, National Institute of Standards and Technology, October 2, 2000.
3. M. Pitchaiah, Philemon Daniel, Praveen “Implementation of Advanced Encryption Standard Algorithm”, International Journal of Scientific & Engineering Research, March 2012; 3(3): ISSN 2229-5518.
4. Alatas B., Akin E., and Ozer A., “Chaos Embedded Particle Swarm Optimization Algorithms,” Chaos Soliton and Fractals Journal, 2009; 40(4): 1715-1734.
5. Lorenz N., “Deterministic Non Periodic Flow,” AMS Journal, 1963; 20(2): 130-141.
6. Petra Snaselova and Frantisek Zboril, “Genetic Algorithm using Theory of Chaos”, Procedia Computer Science, ICCS 2015 International Conference on Computational Science, 2015; 51: 316–325.

7. Champakamala B.S., Padmini K, Radhika, "Least Significant Bit algorithm for image steganography" International Journal of Advanced Computer Technology (IJACT) ISSN: 2319-7900.
8. International Journal of Optics http://dx.doi.org/10.1155/2016/2053724, Research Article: Digital Image Encryption Algorithm Design Based on Genetic Hyperchaos, 2016(2016): Article ID 2053724, 14 pages.
9. Graps, "An Introduction to Wavelets", IEEE Computational Sciences and Engineering, 1995; 2(2): 50-61.
10. M. Naor and A. Shamir, "Visual cryptography", Advances in Cryptology - Eurocrypt' 94, 1994; 950: 1–12.
11. Chandrasekhara and Jagadisha, "Secure banking application using visual cryptography against fake website authenticity theft", International Journal of Advanced Computer Engineering and Communication Technology, 2013.
12. E. E. Jebamalar Leavline, D. Asir Antony Gnana Singh, "Salt and Pepper Noise Detection and Removal in Gray Scale Images: An Experimental Analysis, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No.5 (2013), pp.343-352 http://dx.doi.org/10.14257/ijsip.2013.6.5.30
13. Prabhjot kour, "Image processing using Discrete wavelet transform", IPASJ International Journal of Electronics & Communication (IIJEC) Web Site: http://www.ipasj.org/IIJEC/IIJEC.htm, January 2015; 3(1): ISSN 2321-5984.
14. Yogita Patil, "Use of Genetic Algorithm and Visual Cryptography for Data Hiding in image for Wireless Network", International Journal of Computer Applications (0975 – 8887), March 20; 113(1).