I J C T A, 9(25), 2016, pp. 95-112 ISSN: 0974-5572

Image Steganography Based on Hybrid Discrete Wavelet Transform with Gabor Filter and Optimized Genetic Algorithm

G. Sudha Devi* and K. Thangadurai**

ABSTRACT

Steganography is the process of hiding data within a covering such that it seems similar to a plain covering even though it has concealed information. Steganographic schemes have several challenges like high hiding capacity and imperceptibility. Existing techniques have some complications like less robust and low hiding capacity. State the objectives of the study For the purpose of avoiding the above mentioned complexities, a novel digital image security approach is designed that combines Hybrid Discrete Wavelet Transform and Gabor Filter (HDWT-GF) algorithm and image encryption based on optimized chaotic that is received through Genetic Algorithm (GA) with high degree of reliability and security. It makes use of image as cover media for the purpose of embedding secret image. In this scheme, the entire input and cover images are denoised by means of Non-Local Means (NLM) filtering and preprocessed with the help of Histogram Equalization (HE). After that, the embedding coefficient region is recognized with the assistance of Spatial Fusion Algorithm (SFA). SFA decides the region of embedding is using threshold from the image for the purpose of embedding the encrypted data. Subsequently, the HDWT-GF is applied to embed the cover image in that specific region of input image. The cover image is converted through integer wavelet transform to get hold of four subbands: low-low (LL), low-high (LH), high-low (HL), and high-high (HH). Then, the HDWT scheme is utilized to conceal the secret details present in the wavelet coefficients corresponding to the entire four subbands. For the purpose of enhancing the security related to the concealed information, this scheme initially alters the difference among two wavelet coefficients belonging to a pair and subsequently utilizes the altered difference in order to conceal the data. The difference is computed by means of score normalization method. This proposed work creates the secret information extraction from the stego image more complicated even in case the steganography scheme not succeeds. The proposed scheme significantly outperforms existing techniques in terms of the parameters like Normalized Correlation (NC), Peak Noise to Signal Ratio (PSNR) and Correlation Coefficient (CR) are utilized to assess the clarity, reliability and security of algorithm. The scheme proposed outperforms other steganography schemes with respect to the security of the confidential data and not exposing the potential of covered image.

Keywords: Steganography; Genetic Algorithm; Hybrid Discrete Wavelet Transform; Spatial Fusion Algorithm.

1. INTRODUCTION

With the soaring interest corresponding to the privacy and security, a requirement for several data hiding schemes prevails, which leads to the evolution of different schemes for the purpose of embedding and extraction. Steganography is the most powerful scheme of secret information embedding for coverting communication [1]. Steganography is a process of confidential data hiding in the covered media. In case of image steganography, the media utilized for covering is actually an image and also the image confided is probably an image or some text. Image is a preferred one when compared to rest of the media since its redundant information is more. The most frequently utilized cover media like text, audio, video, images

* Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Karur, Tamilnadu, India, *Email: sudhadeviresearch@gmail.com*

** Assistant Professor and Head of the Department, PG and Research Department of Computer Science, Government Arts College (Autonomous), Karur, Tamilnadu, India.

etc. The most considerable characteristics of steganography are security, capacity and imperceptibility. The most general image steganography schemes are (i) Least Significant Bit (LSB) insertion: The LSB of the image cover are substituted with the following secret details. (ii) Masking and filtering scheme: The particular masking schemes or an analytical formula is utilized to choose particular pixels in order to embed the secret data. This information appears as an essential portion of the image cover following the embedding process. (iii) Transform schemes: The cover image is then modified into transform domain through the process of applying transformation like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Fast Fourier Transform (FFT), Integer Wavelet Transform (IWT), etc. and consequently embedding of secret data into the coefficients that are transformed.

Wavelet transform splits the high and low frequency details on the basis of pixel by pixel. DWT is selected over DCT, since the image in the lower frequency at different levels can provide high resolution [2]. In fact, DWT is then decomposed into Approximation band (LL), vertical band (LH), horizontal band (HL) and diagonal detail band (HH). LL band includes wavelet coefficients of low frequency that hold major portion of the spatial domain image. The remaining bands called as detail bands include high frequency coefficients which encloses the irrelevant edge and part information of the spatial domain image. DWT will permit processing independently free from important perceptible interaction among them and as a result leads to the process imperceptibility have more efficiency. The major applications of steganography include in the domain of digital copy right protection, content authentication, digital media content surveillance and transform communication related industries such as e-pressing, e-government, e-business etc.

Here in this research work, Hybrid Discrete Wavelet Transform and Gabor Filter (HDWT-GF) algorithm is proposed for the purpose of digital image security and image encryption based on optimized chaotic got through GA with large degree of reliability and security. It makes use of image as cover media for the purpose of embedding secret image. At first, Non-Local Means (NLM) filtering is used for denoising the input and cover images. Subsequently, the denoised image is preprocessed by means of Histogram Equalization (HE). Subsequently, the embedding coefficient region is recognized by means of Spatial Fusion Algorithm (SFA). The SFA is using threshold from the image for the purpose of embedding the encrypted data. After that, the HDWT-GF scheme is exploited for the purpose of concealing the secret details present in the wavelet coefficients corresponding to the complete four subbands. In order to obtain enhanced security for the concealed data, the new scheme initially transforms the difference observed between two wavelet coefficients of a pair and subsequently makes use of the difference that is modified for the purpose of concealing the information. The difference is computed by means of score normalization scheme. This yields the secret information extraction from the stego image complicated even when the steganography technique not succeeds.This paper is organized in the sections that follow. Section 2 provides an overview of few related works. The steganography model is described and the algorithms that are employed for the embedding and extraction process in section 3. Section 4 discusses the performance analysis in section 4 and conclusions are given in section 5.

2. RELATED WORK

Ghoshal and Mandal, [3] formulated authentication scheme which discloses the scheme of colour image authentication in the frequency domain dependent on the DFT. DFT is implemented on the sub-image block referred to as mask having size 2×2 for the frequency constituents of the respective spatial module. These convert procedure is carried out from the start to end mask in row major arrangement of the carrier image. Authentication of Image is carried out by means of concealing confidential data into the converted frequency modules corresponding to the carrier image. The four secret message bits are embedded inside the converted real frequency module of every carrier image byte not including the LSB of initial frequency component of every mask. Following THE embedding process, a delicate readjust phase is integrated in the

entire frequency module of every mask, to maintain the quantum value as positive and non-fractional in the spatial domain.

Adel Almohammad and Chinea [4] formulated two steganography schemes JSteg and JMQT which are utilized to examine the pros as well as the cons of color and grayscale versions of the images that are employed in the form of steganography covers. It assesses the performance of both the grayscale and colour versions of a particular cover image while they are utilized with a particular steganography scheme. Thus, colour images are improved rather than when utilizing grayscale images for the purpose of data hiding. With the aim of increasing the hiding capacity, chrominance modules can be utilized for the purpose of data hiding. Elham Ghasemi et al., [5] formulated an embedding scheme with the assistance of mapping function in accordance with GA. The cover image is then partitioned into 8×8 blocks and then transformed with the assistance of IWT. The data is afterwards, embedded into coefficients related to cover image. GA and optimal pixel adjustment offers optimal mapping functionality in order to lessen the error difference among the cover and also the stego image and to aid in enhancing the hiding capability with low distortion correspondingly.

Swain [6] proposed secure communication scheme by the combination of cryptography and image steganography. The confidential data is then encrypted and afterwards embedded in the sixth, seventh and eighth LSB position of the darkest and the brightest pixel that is arbitrarily spread across. Weiming Zhang et al., [7] formulated a scheme for the purpose of building binary stego codes to perform the LSB embedding in gray-scale signals that could be produced with the help of a covering code by means of the Hamming codes and wet paper codes combination. Cui-ling Jianget al., [8] formulated a steganographic scheme in accordance with the adjustment of jpeg quantization tables. Cover image is then partitioned into 16×16 quantization table that is non overlapping. The DCT coefficients are next quantized through quantization table. Secret information is subsequently embedded within the cover image's DCT coefficients. Yan-ping Zhang et al., [9] formulated an effective approach for the purpose of information hiding that result in static digital images in accordance with Hamming Code and Wet Paper Codes. It is through the procedure corresponding to the embedding of seven confidential bits within a pixel set of many cover pixels one at one time, in case that is ineffective, in that scenario, it does the embedding of the first three confidential bits again into that pixel-group.

Septimiu Fabian et al., [10] formulated a scheme with the help of cryptographic algorithms, which are Ron Rivest Adishamir Len Adleman (RSA) algorithm having asymmetric keys and Advanced Encryption Standard (AES) having symmetric key in cooperation with steganography. The integration of the three schemes builds a communication system based on a strong steganography. The confidential information is then encrypted by means of AES with the help of strong key before getting embedded with a Steganographic algorithm. The key utilized for performing the encryption of data makes use of collaboration between a randomly generated sequence and a hash of the color information of the cover image which stays unaffected throughout the complete embedding process.

Chen Gouxi et al., [11] formulated a technique where the marginalization of the cover image is carried out and rebuilt through mathematical based morphology and also block markers, subsequently doing the embedding of the confidential information within the cover image effectively with the help of F5 Steganographic scheme. The scheme yields benefits like the small transformations in quality of image, strong capability in anti-attack, and also the secretive details can be obtained entirely from the carrier image. Anita Christaline and Vaishali [12] formulated a technique consisting of two schemes. First one is filter scheme for the purpose of embedding the text information into the image. The second scheme refers to a wavelet transform scheme which demonstrated to be provide more security rather than any other approach corresponding to image steganography.

Wien Hong and Tung Shou Chen [13] have formulated data-hiding scheme in accordance with matching of pixel pair and makes use of the pixel pair values in the role of a reference coordinate, and searches for a

coordinate present in the neighboring group of this pixel pair in accordance with an information digit given. Subsequently, the pixel pair is substituted with the coordinate searched in order to hide the digit. Che-Wei Lee and Wen-Hsiang Tsai [14] have formulated blind authentication scheme in accordance with the secret sharing scheme having a data repair ability for the grayscale images by means of exploiting the Portable Network Graphics (PNG) image. An authorized signal is constructed for every block of a grayscale document image that in turn, in cooperation with the block content that is binarized, is transformed into numerous shares by means of the scheme of secret sharing.

3. PROPOSED METHODOLOGY

In this section, embedding and extraction is carried out with the assistance of HDWT-GF and the embedding region is recognized with the help of SFA with the encryption and decryption process. At first, the input and cover images are denoised by means of Non-Local Means (NLM) and preprocessed with Histogram Equalization (HE). During the embedding phase, the image cover and secret images are considered as input, in which the encryption of the secret image is by means of GA-chaotic encryption algorithm and the output will be the stego image. Following the embedding process, the extraction of the secret image is acquired by using the secret key and inverse wavelet transform.

3.1. Hybrid Discrete Wavelet Transform and Gabor Filter

In existing scheme, the Lifting Wavelet Transform (LWT) is utilized for the purpose of embedding the image. However, it has certain drawbacks like; this scheme is not focused on particular region of coefficients for transformation and it is not appropriate for large matrix transformation, because of this LWT has very low security. In order to overcome these complications, the Gabor filter is introduced in DWT. Hybrid Discrete Wavelet Transform and Gabor Filter (HDWT-GF) are proposed for embedding the input secret image and cover image.

The proposed methodology is continued as follows. Initially, the DWT is used over the input secret and cover image to get hold of its high frequency image component, because it often includes most of the secret information. Subsequently, a bank of Gabor filters having diverse scales and orientations is utilized over the image with high-frequency in order to get hold of Gabor-filtered images in diverse spatial orientations.

3.2. Discrete Wavelet Transform

The two-dimensional discrete wavelet transform (2D-DWT) [15] carries out a subband coding of an image, by means of an iteration and recursion based process. Figure 1 demonstrates the case related to two-level

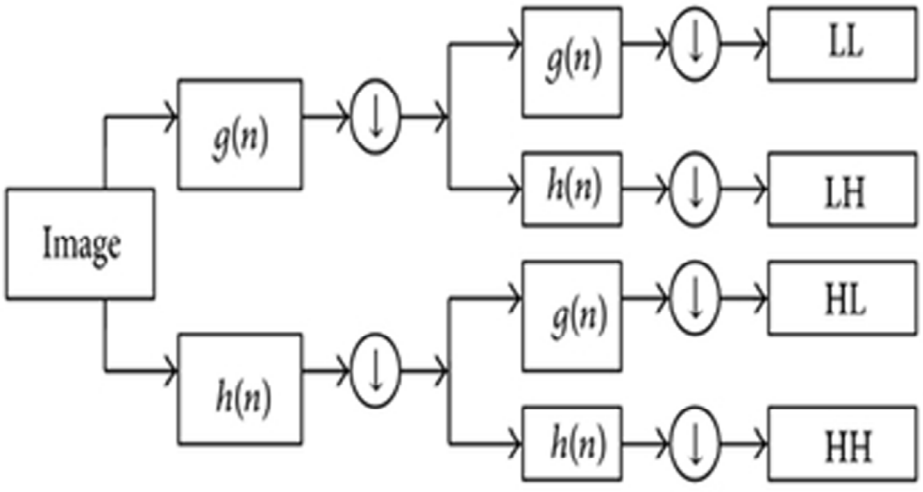


Figure 1: 2D-DWT decomposition of an image

decomposition. The input and cover images are initially represented through LH, HL, and HH subbands which does the encoding of the image characteristics along three directions and an LL subband that renders its approximation. The obtained feature or approximation images could be deconstructed yet again to get hold of detail in the second-level and images of approximation, and the method can be reiterated for enhanced evaluation since every iteration does the doubling of the image scale.

The 2D-DWT computation continues from that received from the 1D-DWT, which is the discrete version corresponding to the one-dimensional continuous wavelet transform. The input pixel of (5ØaÜ) is defined by [16, 17].

$$W_{\psi}(a,b) = \int_{-\infty}^{+\infty} x(t)\psi_{a,b}^{*}(t)\,dt \tag{1}$$

$$\psi_{a,b}(t) = \frac{1}{\sqrt{|a|}}\psi\left(\frac{t-b}{a}\right) \tag{2}$$

Where $\Psi_{a,b}$ (•) specifies a specific wavelet function and indicate the corresponding scale and also translation parameters. The input pixel value is acquired by sampling in order that (1) tends to become that of a sequence. In case of dyadic sampling, a and b are, respective powers of 2 and multiples thence, and also the sequence components (wavelet coefficients) are expressed as

$$C_{jk} = W_{\psi}\left(2^{-j}, 2^{-j}k\right) \tag{3}$$

Where *j* indicates the discrete scale factor and *k* stands for the discrete translation factor. It means, *a* and *b* in (1) are substituted with 2^j and $2^j k$, correspondingly.

The one-dimensional wavelet decomposition is then extended as an image by means of using it over the row variable initially and subsequently over the column variable related to the consequent result. During every step, two sub images are generated having half the pixels number present in the row or column which was processed. During the end, a M × N image is then separated into 4 sub images, having M/2 × N/2 resolution and the preserved scale. On the contrary, (1) has got only merit of theory because of the ranges of a and b that are infinite. During a real-time realization, the fact concerned is (1) is fundamentally a correlation measure between a signal and several wavelets that are got from a mother is made use, and the DWT decomposition is then modified into a filtering process consisting a sequence having high-pass and low-pass filters [18]. Based on the notation in [16, 17], the discrete notation of (1) can be given as,

$$ca_{j,k}\left[x(t)\right] = DS\left[\sum x(t)\,g_j^{*}\left(t-2^j k\right)\right] \tag{4}$$

$$cd_{j,k}\left[x(t)\right] = DS\left[\sum x(t)\,h_j^{*}\left(t-2^j k\right)\right] \tag{5}$$

Where coefficients $ca_{j,k}$ and $cd_{j,k}$ point out approximation and particulars of components output by the respective impulse responses of (n) low-pass and h(n) high-pass, and then the DS operator executes down sampling through a factor of 2. The 1D wavelet decomposition is then expanded to 2D objects by making use of row and column decompositions as indicated in Figure 1. Here in this research, the wavelet [19] that is most often utilized is employed for the purpose of extracting the HH image component.

3.3. Gabor Filter

Here, the two-dimensional Gabor filter does the image decomposition into components at the level of several scales and orientations [20], as a result capturing visual features like spatial localization, selectivity, and spatial frequency. The 2D Gabor filter includes a complicated exponential that is centered at a particular

frequency and then modulated through a Gaussian envelope. As a result of using the complex exponential, the filter contains both the real and imaginary constituents. The general expression of the real part is given as:

$$G\left(x, y, \sigma_x, \sigma_y, f, \theta\right) = \exp\left[-\frac{1}{2}\left(\left(\frac{x'}{\sigma_x}\right)^2\left(\frac{y'}{\sigma_y}\right)^2\right)\right] \tag{6}$$

$$x\cos\left(2\pi f x'\right) \tag{7}$$

Where $x' = x\cos(\theta) + y\sin(\theta)$, $y' = y\cos(\theta) - x\sin(\theta)$, and where σ_x and σ_y represent the standard deviations with respect to the Gaussian envelope in the direction of the *x* and *y* axes. The parameters *f* and θ are, corresponding to the central frequency and also the Gabor filter rotation. With the aim of obtaining the Gabor-filtered image (*x*, *y*) corresponding to a particular image (*x*, *y*) the operation of 2D convolution (*) is then carried out:

$$f\left(x, y\right) = G\left(x, y, \sigma_x, \sigma_y, f, \theta\right) * i\left(x, y\right) \tag{8}$$

The choice of parameters σ_x, σ_y, f and θ plays a significant part in the operation of the filter. On the contrary, no formal scheme exists for deciding on them and experience-led insight, trial and error, or else heuristic search should be exercised. For input secret images and cover images, σ_x and σ_y were set to unity arbitrarily. In this scheme, σ_x and σ_y were fixed to the values, which were decided empirically. As a result, here used $\sigma_x = \tau/2.35$, where τ indicates the complete width at half-maximum value with respect to the Gaussian and $\sigma_y = 8\sigma_x$. None of the values of σ_x and σ_y except the earlier ones were given a try because optimality was not of the significant concern and acquired adequate outcomes with these values. Four orientations, $\theta = 0, \pi/4, \pi/2$, and $3\pi/4$. These values were sensible in the form of a first attempt, as they had covered both the image axis directions and also the forward, backward diagonals. At last, the central frequency f was then fixed to 2, 2.5, and 3. Provided that the Gabor filter is been modulated through the cosine of f,

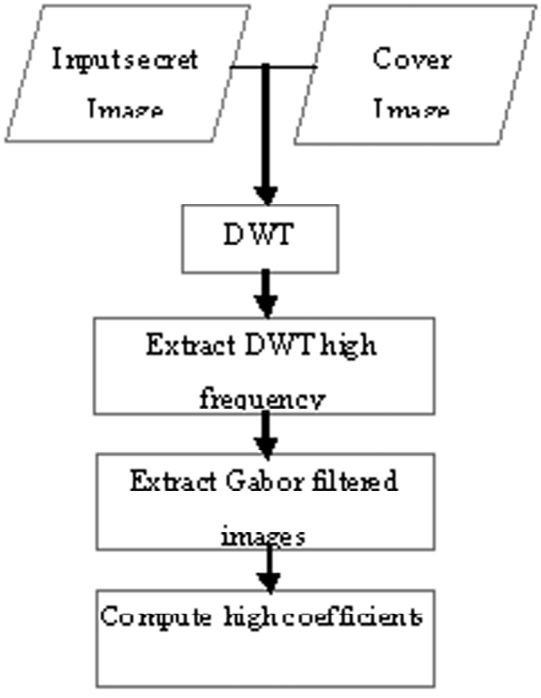


Figure 2: Schematic diagram of the DWT-Gabor approach

big values of f result in a cosine that is compressed and, as a result, the output of the filter has more chances to demonstrate rapid or frequent transformations in embedding the image. Finally, Applying the Gabor filter bank over the HH image component acquired with the 2D-DWT happens to be twelve Gabor-filtered HH images components, for every selection of *f* and θ.

3.4. Image denoising using NLM

The non-local means denoising scheme replaces every pixel in the noisy image through the weighted average of pixels with associated surrounding neighborhoods. The weighting function is decided through the similarity among neighborhoods. In this scheme, it initially computes the similarity among the window centered on a pixel and the window centered on other pixels in the noisy image. The scheme makes use of the similarity to calculate the weighting function. Here, the image is presumed to be distorted by Gaussian white noise with zero-mean and variance δ^2. The observation image model can be taken as given below,

$$V(i) = X(i) + N(i) \tag{9}$$

Given a discrete noisy image = $\{v(i)\ i \in I\}$, where I indicates the image domain. For a pixel *i*, the estimated value is given as,

$$NL[v](i) = \sum_{j \in I} w(i, j) v(j) \tag{10}$$

Where $w(i, j)$ is decided by the similarity observed among the pixel *i* and *j*, and meet the usual conditions $0 \le w(i, j) \le 1$ and $\sum_{j \in I} w(i, j) = 1$. $w(i, j)$ is given as,

$$w(i, j) = \frac{1}{C(i)} \exp\left(-\frac{d(i, j)}{h^2} \right) \tag{11}$$

Where $C(i)$ indicates the normalizing constant and it is given as,

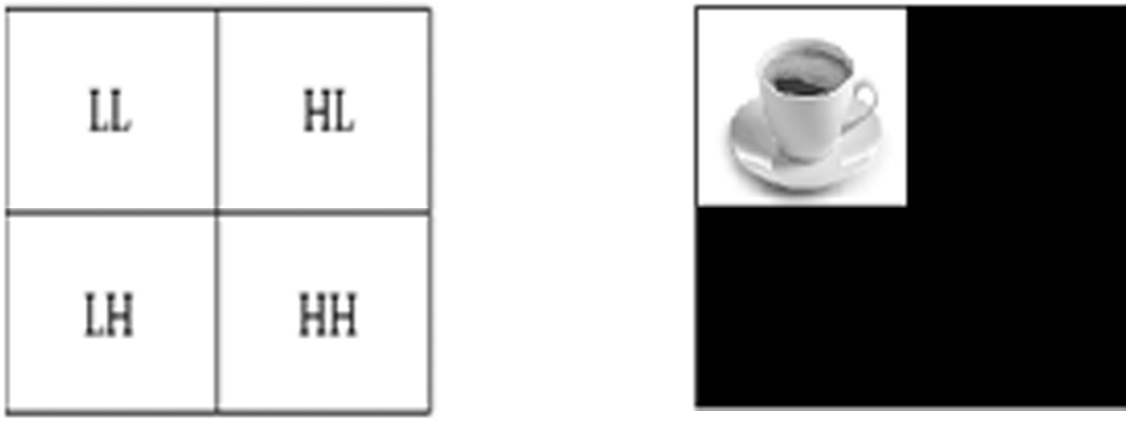
$$C(i) = \sum_{j \in I} \left(-\frac{d(i, j)}{h^2} \right) \tag{12}$$

$$d(i, j) = \left\| v(N_i) - v(N_j) \right\|_{2,a}^2 \tag{13}$$

And *a* indicates the standard deviation corresponding to the Gaussian kernel, *h* represents the decay parameter; it manages the decay with respect to the exponential function. N_i stands for a square neighborhood of fixed size N × N centered at pixel *i*, and $v(N_i)$ indicates the intensity gray values of *v* at N_i. The resulted denoised image is utilized for preprocessing.

3.5. Preprocessing

The gray scale image is taken in the form of a 2D array having size [*M*, *N*]. Initially, histogram modification [21] is done to keep away from the likely overflow/underflow of pixel values. This complication takes place while the pixel values with respect to the cover image are about to 255 or 0, since they might go beyond 255 or slip under 0 at some point in inverse integer wavelet transform. The complication can be resolved by means of mapping of the 15 gray scale levels that are the lowest to the value of 15 and then the uppermost 15 gray scale levels to the value of 240 respectively. When the values of the pixel go beyond the boundaries at some stage in the inverse wavelet transform, the image doesnot hold appropriate for secret data hiding. The image is converted by means of hybrid wavelet transform to get hold of four subbands: LL, LH, HL, and HH having



(a) (b)

Figure 3: (a) Arrangements of wavelet coefficients, (b) The image tea cup after performing hybrid wavelet transform

size] [M/2, N/2] each. The entire four subbands are utilized for the purpose of concealing the secret data. The 2D array having size [M, N] is constructed once more through the process of organizing the four subbands as indicated in Figure 3a. Figure 3b illustrates the four subbands arrangement of the image lena. tiff following the process of transforming it using hybrid wavelet transform. A hybrid array obtained through the process of organizing the wavelet coefficients of four subbands are illustrated as follows:

3.6. Encryption using Genetic Algorithm Chaotic Map

The Genetic Algorithm (GA) is an effective scheme for optimization and search on the basis of the standards of genetics and natural selection. GA includes five components namely random number generator, fitness evaluation unit and genetic operators for the purpose of reproduction, crossover and mutation processes. The initial population that is necessary at the beginning of the algorithm is basically a collection of strings of number produced by means of the random number generator. Every string is an illustration of a solution for the problem of optimization which is being taken into account. Associated with every string is actually a fitness value (fval) that is computed through the wavelet transform. The reproduction operator carries out a natural selection function called as “seeded selection”. Each string is then copied from one of the sets to the subsequent set in accordance with the fitness values, and the greater the value of fitness, the larger is the probability of a string to be chosen for the subsequent generation. The crossover operator decides the string pairs in an arbitrary manner and constructs new pairs. The mutation operator arbitrarily does the mutation or reversal of the values of bits present in a string. An algorithm phase includes application of the evaluation, reproduction, crossover and mutation processes. A new group of solutions is then generated with every stage of the algorithm.

The image encryption technology that depends on chaos is basically a code encryption scheme which is formulated in the last few years. It considers the actual image in the form of the binary data stream that in accordance with certain encoded mode, subsequently does the encryption of the image using the chaotic signal. The cause that Chaos is suitable for the encryption of image is strongly connected to few of its dynamics features. The chaotic signal comprises of natural concealment, more sensibility towards initial conditions and also to smaller perturbation movement, each of these render the chaotic signal with a capability of unforeseeable for a long time. The security of this encryption system is completely based on the level of approximation among the signal and random numbers which are constructed by secret key stream generator (in other terms, be chaotic). The secret key stream is receiving better security since it uses random numbers, simultaneously, it could be broken easily. Logistic map is an instance for nonlinear equation that can find its application for the experimental mathematic studies successfully. Even though it is uncomplicated, it can represent the entire characteristic of nonlinearity phenomenon. Its function is given as follows,

$$X_{n+1} = f\left(\mu, X_n\right) = \mu X_n\left(1 - X_n\right) \tag{14}$$

Where $\mu \in (3.57, 4)$, $Xn \in (0, 1)$. When $\mu = 4$, subsequently the system lies in chaotic state, and also the sequence which the system generates at present possesses the features with respect to randomness, erotic, and the sensibility to actual value. In addition, the range of it is (0, 1). The entire characteristics can offer an extremely good support for the operation of image encryption.

1) Separate the input image into four equal quadrants as shown in figure 4.

(a) **(b)**

Figure 4: (a) plain image (b) plain image divide to 4 equal parts

2) Execute chaotic function logistic map over individually encrypted pixels to every quadrant of image. Steps for encryption by means of chaotic function wavelet map.

a. Initially, five pixels are then chosen from the first row of every quadrant of image that is supposed to be utilized in order to generate the initial value. At this instant, get encryption key from every quadrant to the image, in this manner, the first member of the population is then generated.

b. In order to get hold of initial value of logistic map function, here used the following equation: $P = [P_1, P_2, P_3, P_4, P_5]$ (Decimal)

c. The given equation is subsequently utilized to transform K into a binary number expressed as given below: $Bin = [P_{1,1}, P_{1,2}, P_{1,3}, ..., P_{2,1}, ..., P_{5,7}, P_{5,8}]$ (Binary)

d. The equation following is applied in order to decide the initial value corresponding to the chaotic map function which is shown below:

$$X_{0+k} = \frac{P_{1,1} \times 2^{39}, ..., P_{2,1} \times 2^{31} ..., P_{5,7} \times 2^{1}, P_{5,8} \times 2^{0}}{2^{40}}$$

e. Where $k = 1, 2, 3, 4$

f. For every portion of the plain image, step 2.b & 2.c is reiterated again.

g. For the purpose of encrypting pixels in every part of plain image, following equation is applied:

$$\text{New Value} = \text{round}\,(X_{ik} \times 255) \otimes \text{old Value}$$

3) Genetic Optimization: In this scheme, GA makes use of crossover operation.

4) Correlation coefficient among pairs of neighboring pixels is utilized to get hold of fitness function.

5) Choice of the Best cipher image is based on the source of computation of the entropy and correlation coefficient. Image includes the maximum entropy and the lowest correlation coefficient is selected in the form of the best cipher image and subsequently this image is transmitted towards the destination.

3.7. Spatial Fusion for region selection

The spatial fusion, based on splitting the components of input image in reference to the range of intensity level to embed I_e. Each region count is defined to forecast the maximum counted region to embed a finite set of possible information I_{ei}. For that, at first the input image M is represented by 1-D row vector organized in ascending order indicated by $MR \in M$. The levels of image $L_i \in M_R$ is determined through thresholding the intensity level of the image vector with the equation given below

$$V_{i=1}^{3} L_i = MI_R\left(l \times i\right) \text{ Where } l = \frac{N}{4} - 1 \tag{15}$$

By comparing the limit L_i, the image is decomposed into different level of images D_d with labeling in accordance with the condition, if $i = 1$, subsequently $d = s$; $i = 2$, then $d = R$; $i = 3$, then $d = Q$ else $d = P$ given by

$$D_d\left(x, y\right) = \sum_{x=0}^{N}\sum_{y=0}^{N} MI\left(x, y\right) < L_i count_i ++ \tag{16}$$

The decomposed regions are composed into single image with the help of following equation,

$$F\left(x, y\right) = \sum_{x=0}^{N}\sum_{y=0}^{N} D_d\left(x, y\right) > 1 \tag{17}$$

The algorithm is extremely uncomplicated, resulted less computation for effective composition and decomposition of the input image. It is utilized in the steganography system for effective selection for region of embedding. The knowledge of the size of region to which M_w belongs is adequate enough to recognize the I_e to make sure the availability of information.

3.8. Difference between wavelets coefficients

For the purpose of concealing the data present in the 2D array, score normalization scheme is utilized. In this scheme, a 2 × 2 pixels block are utilized to generate 3 pairs that are subsequently applied in order to conceal the confidential information. After that, it makes use of the 2 × 3 wavelet coefficients block. The 2 wavelet coefficients introduction in the 2 × 2 block creates two additional pairs. As a result, the score normalization scheme considerably enhances the hiding capability of the cover image.

The difference among two of the wavelet coefficients seen in the pair is utilized to conceal the confidential information. When the difference value is then openly applied to hide the data, it is uncomplicated to have the retrieval of the embedded information in the scenario when the steganography system does not succeed. For the purpose of enhancing the security of the confidential information, this scheme adjusts the difference among the two of the wavelet coefficients as seen in the pair and therefore this adjusted difference is utilized to conceal the confidential data. This enforces additional layer of security thereby making extraction of actual secret data harder from stego image by means of difference values in a direct manner. In this scheme, the pixel coefficients are taken as x_i and its means considered as u, subsequently the standard deviation defined as σ. Hence, the difference of pixel coefficients of $x_i^{'}$ is given as,

$$x_i^{'} = \frac{x_i - \mu}{\sigma}, i \in 1,\ 2,\ 3,\ 4,\ 5,\ \ldots \tag{18}$$

From the difference of the entire pixel coefficients, here considered the highest coefficient value for the purpose of embedding process. The highest coefficient value is utilized for HDWT-CF transformation of input secret image embedding process.

3.9. Embedding Procedure

Here, presented the algorithm applied for gray scale images of dimension 256 × 256. The human eye possesses diverse visual sensitivities for different frequencies. Low frequency component are fundamentally utilized for data embedding. For the purpose of higher security, hybrid DWT-CF transform is applied, through which image can be scrambled. In order to embed stego image into original image, Alpha blending is utilized in which the alpha factor is decided (range b/w 0 to 1.0). Consider I represent the original gray scale image of size N × M and secret data in form of image of size M × N. Steps involved in embedding process are given below:

Input: Cover Image (I_C), Secret Image (I_S)

Output: Stego image (I_{stgno})

Step 1: Execute hybrid DWT-CF transform on I_C and I_S with secret Key (K_S) (//*Scrambled Image I_{SS} will be obtained*//

Step 2: Execute 2DLWTDWT on both I_C and Encrypted I_S //* This DWT watermarking can embed only in HL, LH, HH sub bands*//

Step 3: In input image the embedding based on region and difference of coefficients is computed.

Step 4: Extract the approximation coefficient of matrix from HDWT-GF with HL, LH, and HH of level 1 of the I_C and I_{SS}

Step 5: Execute 2D IHDWT-GF (inverse HDWT-GF) to obtain stego image I_{stgno}.

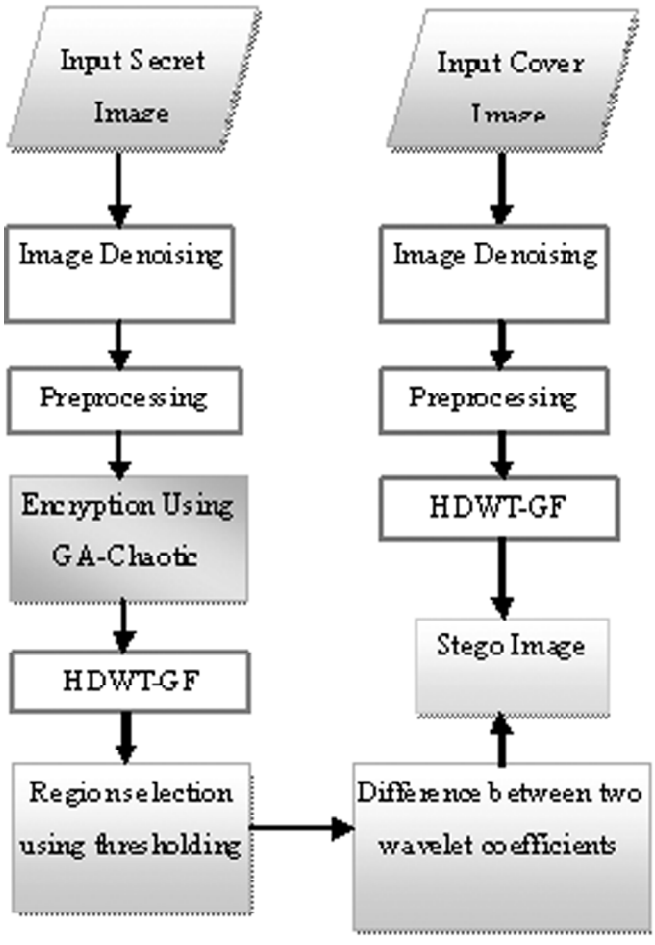


Figure 5: Overall process of embedding procedure

Extraction Procedure

Steps of Extracting Process are as follows:

Input: Cover Image (I_C), stego image (I_{stgno})

Output: Secret Image (I_S)

Step 1: Execute 2-D HDWT-GF of level 1 on both on I_{stgno} and I_C.

Step 2: Carry out IHDWT-GF on separated wavelet coefficients and obtain scrambled secret image.

Step 3: Take inverse Arnold of scrambled secret image.

Step 4: Recovered secret image (which is almost resembling secret image).

4. EXPERIMENTAL RESULTS AND DISCUSSION

The performance of the proposed steganography scheme is implemented by using MATLAB 7.10 version. The comparison parameters for performance evaluation are SC (Structural Content) and NC (Normalized

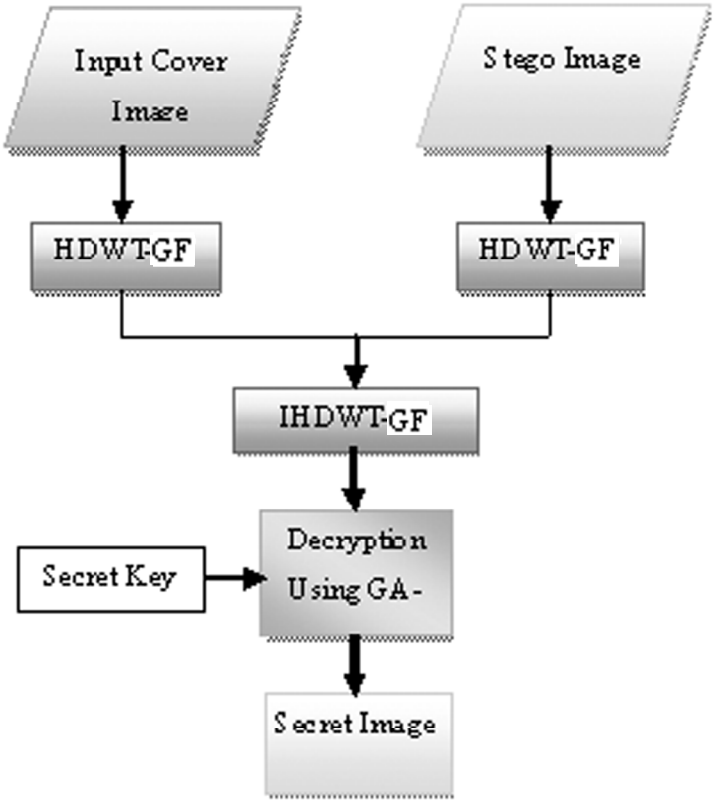


Figure 6: Overall process of extraction process

(a) Car **(b)** **(c) Tea Cup**

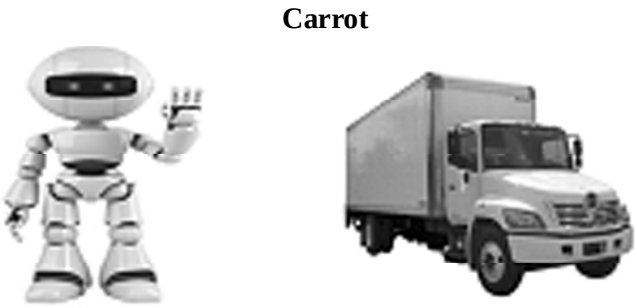


Figure 7: Original test images: (a) Cart (b) Carrot (c) Tea cup (d) Robot (e) Truck

correlation), PSNR, MSE and Cross Correlation. In this experiment, different gray scale images of size 256 × 256 images like car, carrot, tea cup, truck, and robot are taken into account. The six test images utilized for evaluation are given in Figure 7 (a)–(e).

For instance, Figure 8(a) illustrates the cover image as carrot, 8(b) shows the secret image, 8(c) demonstrates the denoised image, 8(d) illustrates the preprocessed image, 8(e) shows the Encrypted Image-chaos with optimized GA, 8(f) shows the Gabor filtered image, 8(g) demonstrates the Stego image, and 8(h) shows the recovered secret image. The experimental results confirms that secret image and recovered secret image are accurately similar to each other as PSNR value is extremely high i.e. 93.75. A better encryption scheme is one where the correlation coefficients among pairs of encrypted neighborhood pixels are placed at the least possible levels. In Figure 9, correlation coefficient is given as -0.0015. Hence, this algorithm also offers higher security. The comparison is done also on the basis of embedding time.

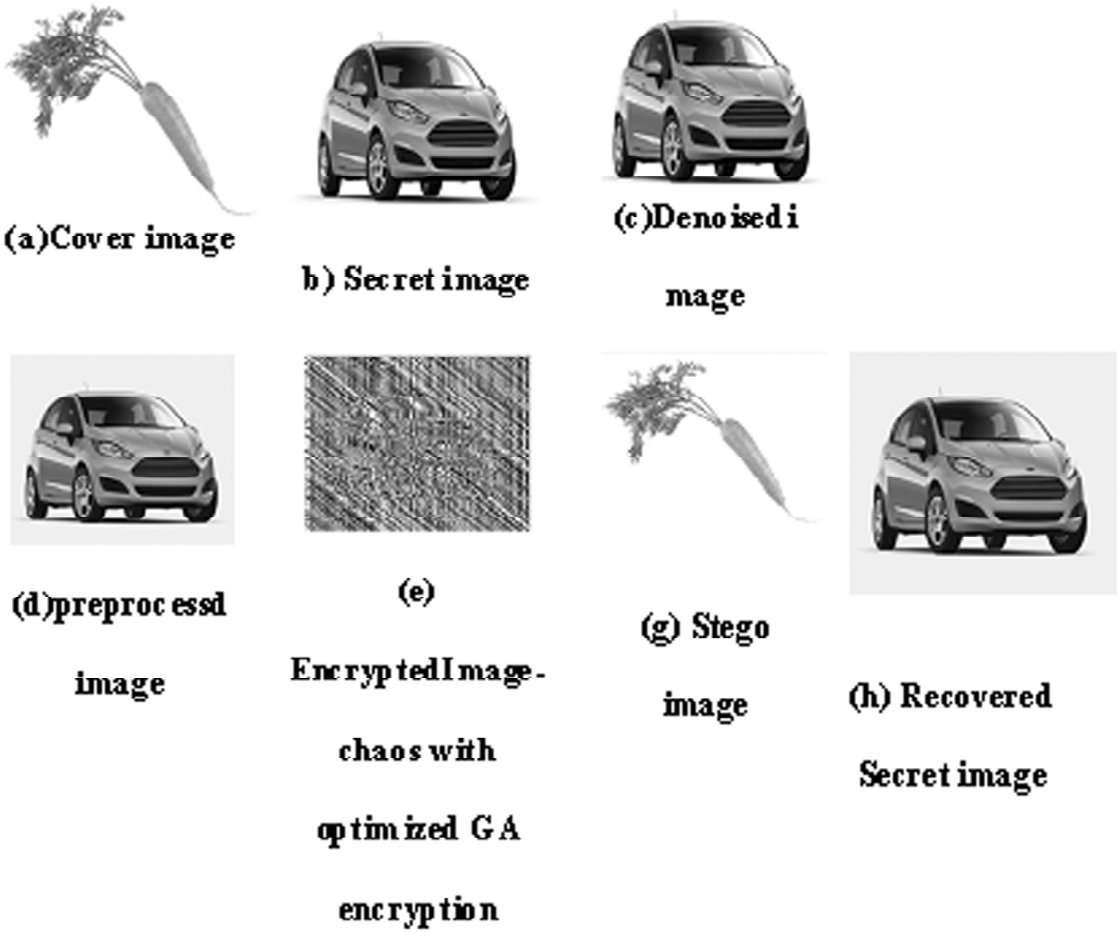


Figure 8: Results after Applying the Proposed Model

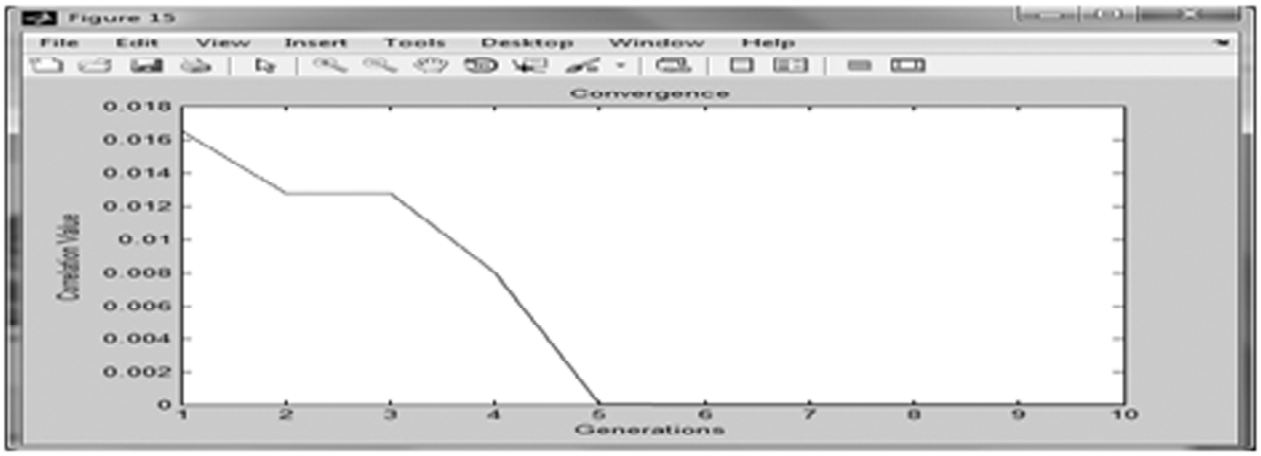


Figure 9: Correlation Coefficient

For several cover image and secret images, the graphs are plotted for the PSNR, MSE, NC and embedding time by values obtained in HDWT-GF based digital image steganography against values obtained in LWT based digital image steganography, using the data from Table-1-2.

Table 1
MSE, PSNR, SC, NC and Time for Proposed GA-Chaotic Map with HDWT-GF

Cover image	*Stego image*	*Hiding capacity (in bytes)*	*MSE*	*PSNR*	*SC*	*NC*	*Time (s)*
Carrot	Car	81142	0.0145	94.50	1.000	0.998	14
Robot	Tea cup	81147	0.0151	94.75	1.000	0.996	13.43
Robot	Truck	81143	0.0147	94.63	1.000	0.995	14.21

Table 2
MSE, PSNR, SC, NC and Time for existing GA-Chaotic Map with LWT

Cover image	*Stego image*	*Hiding capacity (in bytes)*	*MSE*	*PSNR*	*SC*	*NC*	*Time (s)*
Carrot	Car	80121	0.0178	93.43	1.000	0.992	16
Robot	Tea cup	80128	0.0173	93.56	1.000	0.9925	15.89
Robot	Truck	80122	0.0174	93.48	1.000	0.9934	15.92

4.1. Objective analysis-Peak-Signal-To Noise Ratio

As, a performance measure corresponding to image distortion because of embedding, the widely known Peak-Signal-To Noise Ratio (PSNR), that is grouped under difference distortion metrics, could be used for the evaluation of stego images. The good visual quality with respect to the stego images is the most significant property of steganography system since it is complicated to detect by detectors. It is given as:

$$PSNR(dB) = 10\log_{10}\left[\frac{255^2}{MSE}\right] \tag{19}$$

A huge PSNR value indicates that the stego image is most close to original image and vice versa. It is complicated for the Human eyes to differentiate among the actual cover image and the stego image when the PSNR ratio is in excess of 30db. Figure 10 shows a graph of PSNR comparison among proposed scheme and existing scheme. It is obvious from the graph that, at a specific time PSNR value is increased

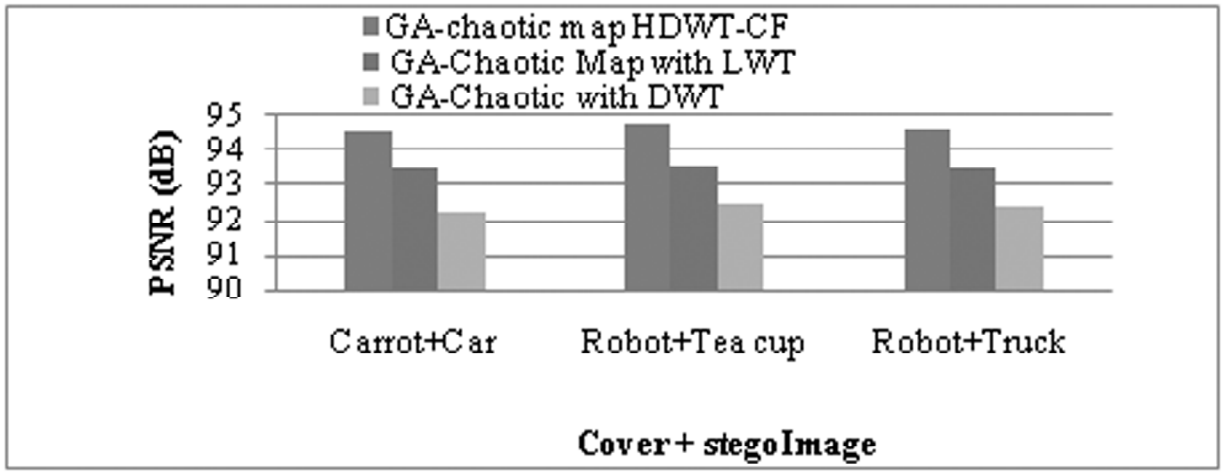


Figure 10: PSNR Comparison Results

in the proposed scheme. Both cannot have maximum at same time. In proposed method PSNR is 78.35 dB that is good which is higher than existing approach. This graph shows that the proposed method gives good PSNR.

4.2. Mean Square Error

MSE refers to the mean square error indicating the difference among the actual cover image I_c sized as M × N and the stego image I_s sized as M × N.

$$MSE = \frac{\sum_{\forall(m,n)} \left[I_C(m,n) - I_S(m,n) \right]^2}{m \times n} \tag{20}$$

Figure 11 demonstrates a graph of MSE comparison among proposed approach and existing approach. It is obvious from the graph that, at a particular time MSE value is decreased in proposed method. Both cannot have maximum at same time. This graph shows that the proposed technique yields good PSNR.

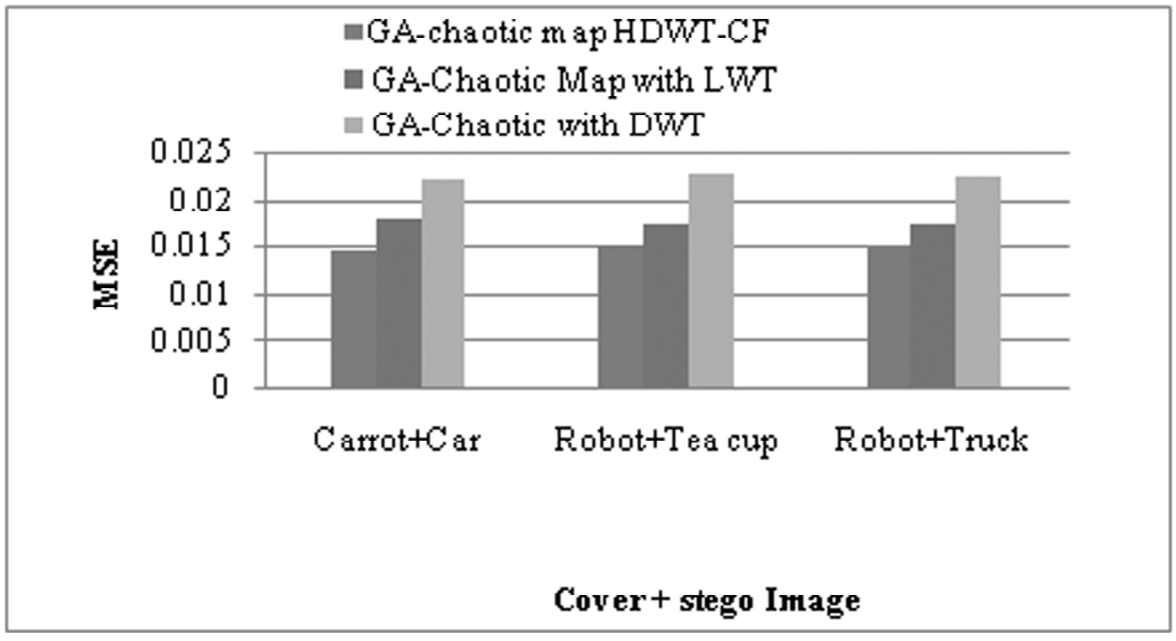


Figure 11: MSE Comparison Results

4.3. Normalized Correlation (NC)

NC (Normalized Correlation) parameter is exploited to assess the reliability of the scheme proposed. In order to find the robustness, following the process of extracting the secret image, similar measurement of the extracted and the cover image are utilized as validation. It can be defined by NC as given below:

$$NC = \sum_{\forall(m,n)} \left(\frac{I_C(m,n) \times I_S(m,n)}{\left(I_S(m,n)\right)^2} \right) \tag{21}$$

4.4. Structural Content (SC)

SC is also correlation based measure and measures the similarity present between two images. Structural Content (SC) is given by the equation:

$$SC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} \left(w'(i,j) \right)}{\sum_{i=1}^{N} \sum_{j=1}^{N} w(i,j)} \tag{22}$$

4.5. Correlation Coefficient

The Correlation Coefficient respective to two similar size images also tells the similarity between the images. In case the value of Correlation Coefficient is close to 1, then two images are very identical. In case the value is 1 i.e. both images are same. Here we use it to compute the similarity measurement of original secret image and recovered secret image, which is expressed as

$$corrcoeff = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} \left(w(i,j) * w'(i,j) \right)}{\sum_{i=1}^{N} \sum_{j=1}^{N} w^2(i,j)} \tag{23}$$

Where N × N is the size of secret image, $w(i, j)$ and $w'(i, j)$ denotes the original and recovered secret images respectively.

4.6. Embedding Time

Figure.12 shows the processing time for embedding the information compressed using HDWT-HF based technique and LWT based technique. From the figure 12, it is noted that the processing time for the proposed

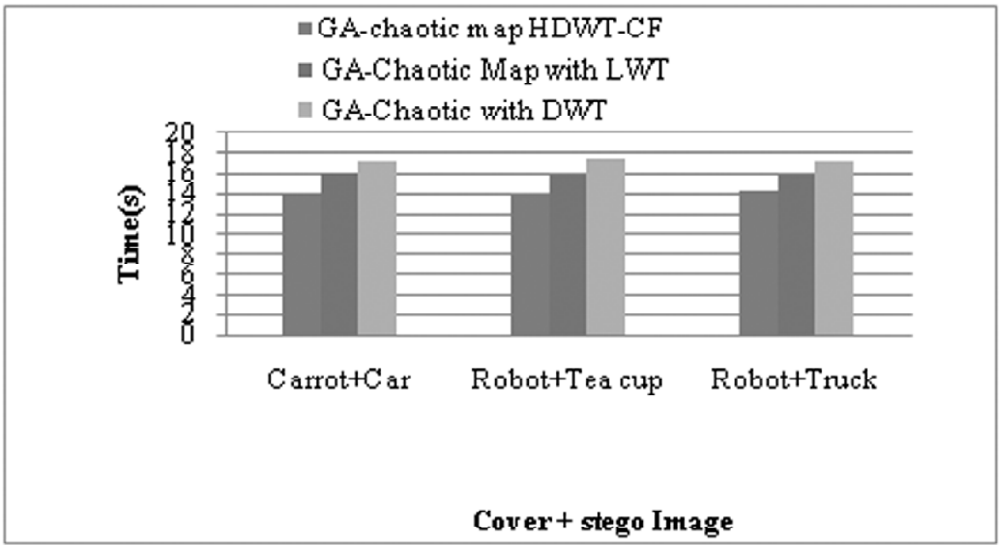


Figure 12: Time Comparison Results

work is less when compared to existing approach. At the same time, the proposed method results in good visual quality of the stego image with perceptual invisibility of the secret image and high security.

5. CONCLUSION

In the field of steganography, hiding capability of the cover image, quality with respect to the stego image, and the security of the confidential data are the three vital aspects that must considered. A trade-off is observed always to be existing among data hiding capability of the cover image and secret data security. The proposed scheme offers enhancements in the data concealing capability in addition to the security of the confidential data in comparison against GA chaotic map with LWT and GA-Chaotic Map with DWT schemes. The input and cover images are denoised by means of Non-Local Means (NLM) filtering and preprocessed with the help of Histogram Equalization (HE). Subsequently, the embedding coefficient region is recognized with Spatial Fusion Algorithm (SFA). Even though the proposed scheme yields better PSNR values in comparison against exiting scheme, the proposed scheme considerably enhances the security of the confidential information. The secret data is hidden securely in the coefficients of HDWT with Gabor filter. For the ease of implementation, the four subbands received after the decomposition of the cover image by means of HDWT-GF. When the steganography technique does not succeed, accurately estimating the number of bits which are hidden for few of the pairs will then be a problem for the intruder. As a result, one another degree of security is enforced for the purpose of securing the secret information. The result obtained and proves that this scheme has more efficiency when compared with other schemes for image encryption. In future to come, this model has to be extended for use in the processes of medical image and medical report transaction.

REFERENCES

[1] K. Thangadurai and G. Sudha devi, “An analysis of LSB Based Image Steganography Techniques, International conference on Computer Communication and Informatics”, (ICCCI), IEEE, pp. 1-4, 2014.

[2] G. Sudha devi and K. Thangadurai, “A Robust and High Secure LWT based Image Steganography and Optimized Genetic Algorithm based Chaotic Encryption Approach”, International Journal of Applied Engineering Research. International Journal of Applied Engineering Research, Vol. 10, No. 12, pp. 32477-492, 2015.

[3] N. Ghoshal and J.K. Mandal, “A Steganographic Scheme for Colour Image Authentication”, IEEE International Conference on Recent Trends in Informa-tion Technology, pp. 826-31, 2011.

[4] A. Almohammad and G. Ghinea “Image Steganography and Chrominance Components”, IEEE International Conference on Computer and Information Technology, pp. 996 – 1001, 2010.

[5] E. Ghasemi, J. Shanbehzadeh and B. Zahir Azami, “A Steganographic Method Based on Integer Wavelet Transform and Genetic Algorithm”, International Conference on Communications and Signal Processing, pp. 42-45, 2011.

[6] G. Swain and S.K. Lenka, “A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels”, International Conference on Communication and Computational Intelligence, pp. 529- 34, 2010.

[7] W. Zhang, X. Zhang and S. Wang, “Near-Optimal Codes for Information Embedding in Gray-Scale Signals”, IEEE Transactions on Information Theory, pp. 1262-70, 2010.

[8] C.L. Jiang, Y.L Pang and Y.A. YuZhu, “Steganographic Method based on the JPEG Digital Images”, Third International Conference on Computer Research and Development, 2011, pp. 35-38.

[9] Y.P. Zhang, J. Jiang, C. Xu and X.Y.H.B, Chen, “A New Scheme for Information Hiding Based on Digital Images”, Seventh International Conference on Computational Intelligence and Security, Hainan , pp. 512 – 16, 2011.

[10] S. Fabian, M.M. Vladutiu and L. Prodan, “Secret Data Communication System Using Steganography”, AES and RSA, Seventeenth International Symposium for Design and Technology in Electronic Packaging, pp. 339 – 44, 2011.

[11] C. Gouxi, C. Min, F. Donglai and M. Qiaomei. “Research on An Stega-nographic Algorithm Based on Image Edge”, International Conference on In-ternet Technology and Applications, Wuhan, pp. 1- 4, 2011.

[12] J. Anita Christaline and D. Vaishali “Image Steganographic Techniques with Improved Embedding Capacity and Robustness”, International Conference on Recent Trends in Information Technology, pp. 97 -101, 2011.

[13] W. Hong and T.S.A, “Chen Novel Data Embedding Method Using Adaptive Pixel Pair Matching “, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 176-88, 2012.

[14] C.W. Lee and W.H. Tsai, "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability", IEEE Transactions on Image processing, Vol. 21, No. 12, pp. 207-18, 2012.

[15] M. Vetterli and C. Herley, "Wavelets filter banks: theory and design", IEEE Transactions on Signal Processing, Vol. 40, No. 9, pp. 2207–32, 1992.

[16] Y. Zhang, S. Wang and L. Wu, "A novel method for magnetic resonance brain image classification based on adaptive chaotic PSO", Progress in Electromagnetic Research, Vol. 109, pp. 325–43, 2010.

[17] Y. Zhang, Z. Dong and L. Wu, Wang S, "A hybrid method for MRI brain image classification", Expert Systems with Applications, Vol. 38, No. 8, pp. 10049–053, 2011.

[18] S.G. Mallat, "Theory formultiresolution signal decomposition: the wavelet representation", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 11, No. 7, pp. 674–93, 1989.

[19] J. Ma and G. Plonka, "The curvelet transform: a review of recent applications", IEEE Signal Processing Magazine, Vol. 27, No. 2, pp. 118–33, 2010.

[20] R.J. Ferrari, R.M. Rangayyan J.E.L. Desautels, and A.F. Frere, "Analysis of asymmetry in mammograms via directional filtering with Gabor wavelets", IEEE Transactions on Medical Imaging, Vol. 20, No. 9, pp. 953–64, 2001.

[21] G. Xuan, Y.Q. Shi, C. Yang, Y. Zheng, D. Zou and P. Chai, "Lossless data hiding using integer wavelet transform and threshold embedding technique", in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '05), IEEE, Amsterdam, The Netherlands, pp. 1520–23, 2005.