International Journal of Soft Computing 13 (3): 102-107, 2018
ISSN: 1816-9503

Dynamic Key Visual Cryptography Using Particle Swarm Optimization Hybridized with Differential Evolution

[1]Hare Ram Sah and [2]G. Gunasekaran
[1]Faculty of Computer Science and Engineering, Sathyabama University, Chennai, India
[2]Department of Computer Science and Engineering, Meenakshi College of Engineering, Chennai, India

Abstract: Visual cryptography in modern days is of paramount way of secured way of communicating the secret image. In this study, a novel algorithm Differential Particle Swarm Visual Cryptography (DPSVC) is proposed for generating the secret key. In this approach the particle swarm optimization is hybridized with differential evolution algorithm. Modification of every particles velocity in the swarm by applying the mutation using differential evolution algorithm. Dynamic key generated for visual cryptography of the color shares are based on the solution space using the histogram frequency of the image to be encrypted. This novel algorithm has improved the performance of the visual cryptography by 93.5%.

Key words: Visual cryptography, secret key, optimization, shares, encrypted, performance

INTRODUCTION

The security of data is of paramount issues which made many researchers to explore the most viable options to ensure its confidentiality. Images are easily captured using smart phones and distributed across networks which is used for day to day life and in business perspective. Many approaches have been applied to ensure the confidentiality and privacy of the data in nature. Traditional approaches like DES, AES are not suitable to handle image data. Encrypting every bit of image data is not needed because of redundancy of data and different parts contributing different visual effects. So, multiple schemes have been applied for encrypting image based on the characteristics of the image. Chen *et al.* (2004), Grangetto *et al.* (2006), Mao and Wu (2006). The Visual Cryptography (VC) proposed by Naor and Shamir (1995) and Chen *et al.* (2004) is a technique that transmits a secret image using multiple shares generated from the image to the receiver. The receiver reconstructs the secret image with the shares received by him using decryption strategy. Visual cryptography encrypts the secret image into shares where noises are added to the image in order to improve its security. Visual crypto graphy security depends on the encryption of the shares of the given image. Particle Swarm Optimizations (PSO) algorithm simulates the behavior of animals (Naor and Shamir, 1995) applying group strategies in locating the food. In PSO ,similar to a treasure hunt game where the players share the clue regarding the treasure to their teammates to further explore the path leading to the treasure which is food in the case of animals. Particle swarm optimization algorithm explores the complete solution space and converges to the optimized value in the space. There are two types of PSO namely local PSO and global PSO based on the neighborhood size for knowledge sharing in reaching the solution. In local PSO (Naor and Shamir, 1995) the next position of every particle is obtained from the social velocity component from a small neighborhood which differs from particle to particle. In global PSO method velocity updation of the particle is performed using the leader of the respective iteration. For every particle new position on its journey towards the path of reaching the solution is calculated based on the velocity. The velocity updation has two components namely cognitive and social component. In cognitive component the particle follows its own personal best in choosing the velocity and in social component it follows based on society. The individual particles which are part of the group are one of the representations of solution which has infinite number of such particles to explore to extract the most optimized solution. The neighborhood size (Toreini and Mehrnejad, 2011) and particles can be identified based on certain network structures. In ring network every particle is attached in a circular form with every particle has two adjacent neighbors for receiving the social input for deciding the new velocity. In cluster, Kulkarni and Venayagamoorthy (2011) network individual particles form clusters based on similar properties where the cluster

Corresponding Author: Hare Ram Sah, Faculty of Computer Science and Engineering, Sathyabama University, Chennai, India

head from each cluster acts as the neighbor for the individuals. In complete network all the particles are neighbor to all other particles which represents the global best approach rather than local best approach. Visual cryptography security depends on the encryption of the shares of the given image.

Differential Evolution (DE) is genetic algorithm based optimization approach in extracting the most relevant solution close to the absolute by analyzing the complete solution space. In DE each individual is represented as chromosomes with features as the genes which represent one of the patterns of the population. The features of the image namely the color components namely red, green and blue are part of the chromosome. Differential evolution is one of the flavors of evolutionary approaches where phenotype approach is followed rather than genotype. In this approach new children are produced from the existing population using mutation where each individual chromosome of the current generation modify themselves by using mutation (Catley *et al*., 2006) to become new offspring. Phenotypic approach in this method generates new offspring based on the current population which leads to a new generation better than the existing population which helps in reaching the best solution very quickly reducing the number of iterations. An advanced system of encrypting data that combines the features of cryptography and steganography along with privacy preservation is presented (Quteishat *et al*., 2010). Secure data sharing using visual cryptography with selective retrieval upon key match is introduced (Sah and Gunasekaran, 2014). Steganography and cryptography properties are combined in such a way to make it harder to retrieve the image of the secret message. The image is sliced, the sliced images are stored and upon match with a search string query the original image is retrieved by merging the individual randomly ordered slices in a regular manner. The image slicing ensures privacy preserving and thread based mining reduces the time complexity of the search algorithm Sah and Gunasekaran, (2016). Multithread approach is combined in the searching process to reduce the time complexity of the search algorithm. This method is particularly advantageous to store large number of records, categorized into different groups and each group indexed with specific keys and when used at the receiving side the particular group image (s) becomes accessible (Sah and Gunasekaran, 2015a, b).

MATERIALS AND METHODS

In visual cryptography approach the original image which needs to be encrypted is split into three shares of RGB images. The three shares are encrypted using the

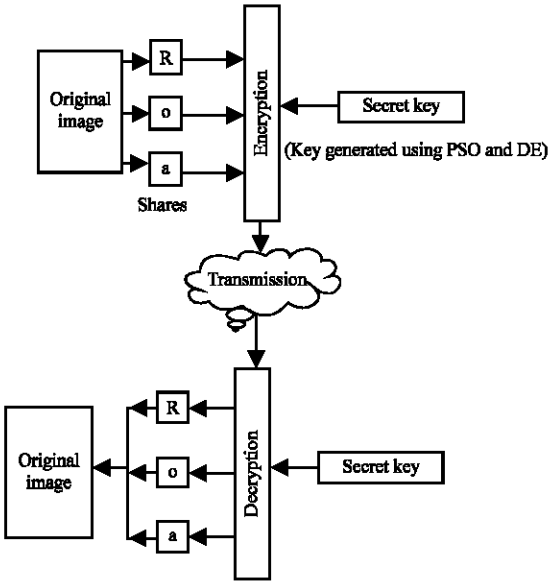

Fig. 1: The architecture of the visual cryptography using secret key for generating shares of RGB

secret key generated from the PSO combine with differential evolution for mutating the velocity of the particles. The overall encryption and decryption of the image is shown in Fig. 1. The encrypted image is transmitted to the receiver. The receiver decrypts the image using the same key for three different shares and combines them to form the original image as shown in Fig. 1.

In Fig. 1 the secret key is generated using the particle swarm optimization algorithm with the differential evolution algorithm. In the particle swarm optimization approach the velocity of the particle is obtained using the differential evolution where new off springs are generated using crossing over and mutation. The secret key for encrypting the image is obtained from the particle swarm optimization and mutation of the particles using differential evolution algorithm. In Particle swarm optimization every particle is represented using the position which consists of the features of the image. The new position of the particle at time t is represented as:

$$X_{ij}(t) = X_{ij}(t\text{-}1) + V_{ij}(t) \quad (1)$$

where, i = 1, 2..., n individuals represents the ith particle and j = 1, 2, ..., m dimensions represents the jth feature of the particle $x_{ij}(t\text{-}1)$ is the old position and $v_{ij}(t)$ is the new velocity at time t.

The velocity of the particle is obtained from cognitive component and social component of the individual and is given by:

$$V_{ij}(t) = V_{ij}(t\text{-}1) + c_1 r_{1j}\left(y_{ij}(t\text{-}1) - X_{ij}(t\text{-}1)\right) + c_2 r_{2j}\left(y^{j}(t\text{-}1) - X_{ij}(t\text{-}1)\right) \quad (2)$$

Where:

c_1 and c_2 = The behavioral amplification constants

r_1, r_2 = The two random numbers simulating the cognitive and the social behaviorism of animals in changing the velocity

$Y_i(t)$ = The individual personal best of ith particle so, far in its journey whereas

Y_t = The global best individual at time t

The evaluation of personal best $y_i(t)$ at time t is evaluated as shown in the Eq. 3:

$$y_i(t) = \begin{cases} X_i(t) & \text{if } f\left(x_i(t)\right) < f\left(y_i(t\text{-}1)\right) \\ y_i(t\text{-}1) & \text{otherwise} \end{cases} \quad (3)$$

Where:

$f(x_i(t))$ = The fitness value of new position obtained for the particle at time

t and $f(y_i(t\text{-}1))$ = The personal best fitness of the ith particle at time t-1

The global best particle at time t represented as y_t is obtained by evaluating the fitness of each particle at its new position and selecting the new leader whose fitness is best among all the individuals. The formula for evaluating the leader is as given. The new best particle at time t is given by:

$$y_t = \min\left\{y_i(t)\right\} \quad (4)$$

where, i = 1, 2, ..., m particles. The velocity (Wang and Zhang, 2011) obtained for every particle is used for calculating the new position of the particle by applying differential evolution in generating new off springs using the trial vector. The trial vector for every particle is obtained by randomly generating two particles x1 and x2 from the population of particles and applying the below Eq. 5:

$$u_{ij}(t) = x_{ij}(t) + \beta\left(x_{1j}(t) - x_{2j}(t)\right) \quad (5)$$

Where:

u_{ij} = The ith particle trial vector and β is the constant to merge the difference between two individuals of the existing population. The value of

β = The taken between 0.5-0.9

The proposed algorithm replaces β with the velocity obtained from PSO, so the equation becomes:

$$u_{ij}(t+1) = x_{ij}(t) + v_{ij}(t)\left(x_{1j}(t) - x_{2j}(t)\right) \quad (6)$$

The proposed Differential Particle Swarm Visual Cryptography (DPSVC) is given as.

Algorithm 1; DPSVC algorithm:

```
DPSVC()
{
Load the image
Extract the color components R, G, B
Normalise()  // Normalise the color components R, G, B
t = 0
generate initial population randomly of m individuals
Initialize velocity of n particles
for every particle xi, i = 1, 2, ..., m individuals
        yi(0) = xi(0)  // Initialize the current position xi(0) for each individual
as its personal best yi(0)
end
while(!terminating condition())
{
for every particle xi, i = 1,2, ..., m individuals
        Evaluate fitness f(xi(t)) based on the input image
        Evaluate individual personal best yi(t+1) using Eq. 3
         Evaluate leader y^(t) using Eq. 4
end
for every particle xi , i = 1, 2, ..., m individuals
        Calculate individual particles velocity vi (t) using Eq. 2
end
DE (velocity, population)
t = t+1
end
 generate the secret key form the best particles
Encrypt the input image using the secret key
 Transmit the encrypted image to the receiver
Decrypt the image using the secret key
}
```

The secret key obtained by the combination of PSO where velocity of the particles is obtained which is used to generate new individuals in differential evolution. The secret key is used for encrypting the image share and transmitted to the receiver. The receiver decrypts the image using the same secret key and combines the share to get the original transmitted image as shown in the Algorithm 1.

Algorithm 2; DE algorithm:

```
DE n (velocity, population)
{
for every particle xi, i = 1, 2, …, m
        Randomly select x1 ≠ xi
        Randomly select x2 ≠ x1 ≠ xi
                for each dimension j = 1, 2, 3, ..., n
                uij(t) = xij(t)+vij(x1(t)-x2(t)); // trial vector ui(t) is
                generated end
                Apply crossing over between xi(t) and trial vector ui(t) using
binomial crossing over algorithm
end
return xi(t)
}
```

DE algorithm is applied in to generate the new offspring by crossing over the individual with the trial vector as shown in the Algorithm 3. Binomial crossing over algorithm is applied in generating the new offspring. In binomial crossing over approach we select the

Normalization: The input image color pixel values are extracted separately as RGB and all the values from 0 to 255 is normalized. The minimum and maximum value of each color component is taken from the image and applied in the below equation to get the required result which is normalized between 0-1:

$$\text{Normalize (pixel)} = (\text{pixel}_{R,G,B}\text{-min})/\text{max} \quad (7)$$

Where min and max are minimum and maximum values of the pixels in arrays of vectors in vertical of the image.

Swarm initialization: The initial swarm of particles in the solution space is randomly generated. The initial population of m particles is generated using uniform random distribution.

Algorithm 3; Swarm initialization algorithm:

For xi = 1, 2, ..., of m individuals
  For j = 1, 2, ..., of n dimension
    $x_{ij}(t)$ = Uniform Distribution(0, 1)
  end
  end

Initial velocity of every particle is initialized with small random values which are uniformly distributed.

Fitness calculation: Fitness of every individual is measured using the Euclidean distance formula between the particles and the training data set. The RGB values of the color image are taken as the features of the image and distance measure results in the fitness of the particle based on the given image. The fitness function is given by the below Eq. 8:

$$\text{Distance}(X, Y) = \sqrt{\sum_{i=1}^{n}(\text{xi-yi})2} \quad (8)$$

Where:

x_i = The components of X vector and
y_i = The components of Y vector

Updating personal and global best: Every individual has so, far experienced the personal best position based on the fitness value. Their personal best is modified based on Eq. 3 by comparing the current position better than its previous best. The global best is the best position enjoyedby the leader of the group. The global best position can also, be updated based on the current positions of the individuals.

Velocity calculation: The velocity of each particle is obtained by applying the differential evolution algorithm is deriving the velocity component. The velocity of each particle vi(t) is obtained by:

- For i = 1, 2, ... of P particles
- For j = 1, 2, ... of m dimension

$$v_{ij}(t+1) = v_{ij}(t)+c_1r_{1j}\left(y_{ij}(t)-p_{ij}(t)\right)+c_2r_{2j}\left(y\text{^}j(t)-p_{ij}(t)\right.$$

The velocity is derived by adding the initial velocity with the social and cognitive velocity components. The constants c_1 and c_2 are initialized with a value between 0 to 1. The random numbers r_{1j} and r_{2j} are generated based on the uniform distribution. The velocity obtained is applied for generating the trial vector in differential evolution for deriving the secret key for encrypting the image.

Applying DE: Catley *et al.* (2006) for each particle xi in the swarm, two unique particles p1 and p2 are randomly selected such that $p1 \neq p2 \neq p_i$. A trial vector is vi(t) is generated for every particle using the formula:

- For p_i = 1, 2, ..., of P particles
- For j = 1, 2, ..., of m dimension

$$v_{ij}(t) = p_{ij}(t)+v_{ij}(t)*\left(p_{1j}(t)-p_{2j}(t)\right.$$

Crossing over of the particle $x_i(t)$ with trial vector $v_i(t)$ takes place where some of the dimensions of particle is replaced by trial vector components to create a new position $x_i(t+1)$ for the particle.

Encryption: The encryption of the visual image is performed by using the secret key obtained from the best particles of the final solution. The top 10% of the best individuals of the population is taken in deriving the secret key for encryption . The range is obtained for each color component of the image by finding the maximum and minimum value of the attributes using the variance of the final best population. The shares are then encrypted using the key and transmitted across the internet to the receiver using standard encryption techniques.

Decryption: The encrypted color image in the form of shares is decrypted using symmetric key generated in the DPSVC algorithm. The encrypted color shares from the R,

G and B components are decrypted using the symmetric key. The original image is obtained by merging all the decrypted color shares of the image. The decrypted image more or less resembles similar to the original image.

RESULTS AND DISCUSSION

Experiment is conducted over more than 1000 images of various image format files. The dynamic secret keys are generated by varying the values of the constants c1 and 2 and results are quite promising. The color image components RGB shares are encrypted using the secret key generated based on DPSVC algorithm.

In Fig. 2, column a represents the original image is encrypted using the two different combinations of c1 = 0.5 and c2 = 0.6 and vice versa. In column b, c and d the RGB colors shares are encrypted using the secret key obtained values of c1 and 2. The first row represents the original image in the column a, red component share of the from the particle swarm optimization for two different original image in the column b, green component share of the original image in the column c and blue component share of the original image in column d. The second row and third row represents the encryption of the shares using secret key obtained from the particle swarm optimization.

Figure 3 and 4 represents of the fitness values of the particles used for generating the secret key with values of c1 = 0.5 and c2 = 0.6 interchangeable for 400 iterations, respectively. Figure 5 and 6 represents of the fitness values of the particles used for generating the secret key with values of c1 = 0.5 and c2 = 0.6 interchangeable for 500 iterations, respectively. When comparing Fig. 5 and 6, we observe that cognitive velocity component is dominating the social component since individual fitness is very high at c1 = 0.6 compared to fitness at c2 = 0.5.

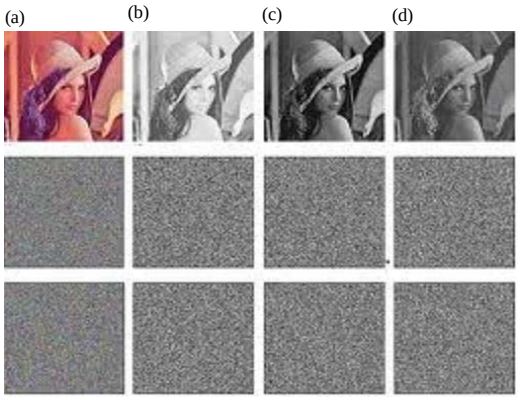

Fig. 2: Encrypted shares of RGB for two different values of c1 and c2

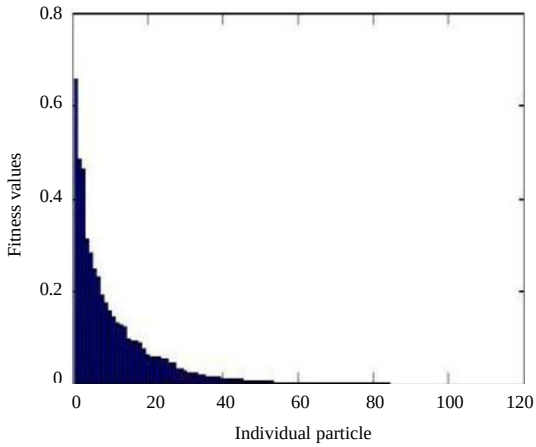

Fig. 3: Particle fitness with the constants c1 = 0.6 and c2 = 0.5 for 400 iterations

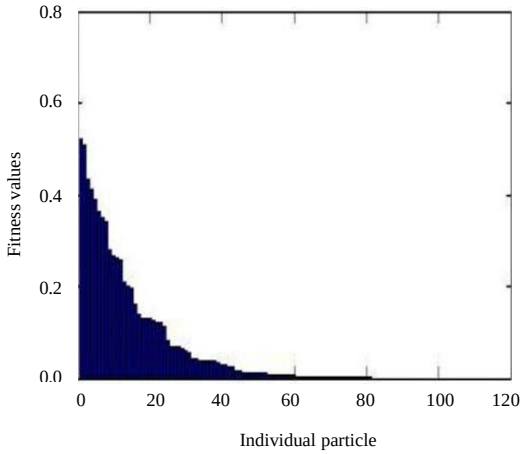

Fig. 4: Particles fitness with the constants c1 = 0.5 and c2 = 0.6 for 400 iterations

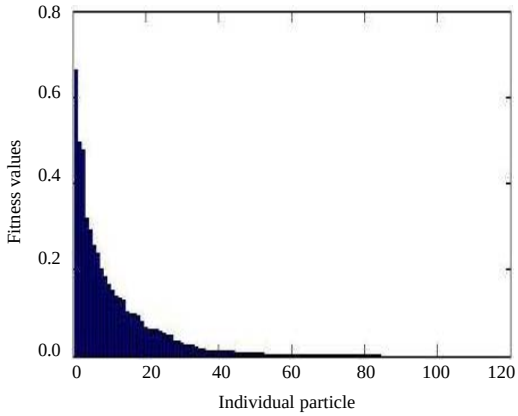

Fig. 5: Particle fitness with the constants c1 = 0.6 and c2 = 0.5 for 500 iterations

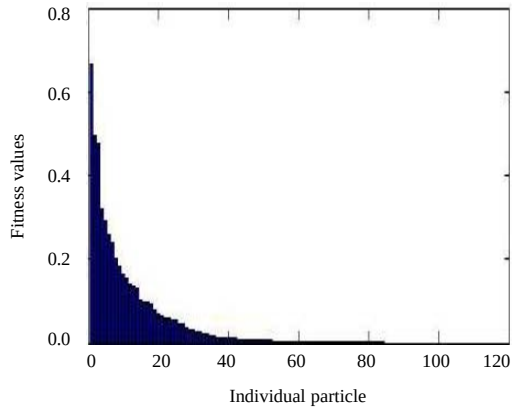

Fig. 6: Particles fitness with the constants c1 = 0.5 and c2 = 0.6 for 500 iterations

CONCLUSION

In this study, a novel visual cryptography algorithm DPSVC is proposed. The research work improves the confidentiality of the encrypted image by 93% by applying dynamic key generated using particle swarm optimization. In this research work there is a hybrid of particle swarm optimization with the merger of differential evolution is applied to increase the confidentiality of the image. Individual encryption of the RGB also adds strength to the encryption. In future you can extend the work towards by applying deep learning algorithms to improvise on the security of the data. Convolution neural networks, deep belief networks, restricted boltzmann network model can be applied on improving the performance of the encryption algorithm.

IMPLEMENTATIONS

The image to be encrypted is split into three shares of colors red, blue and green. The shares are encrypted by using the secret key generated from the pattern evolved from particle swarm combined with differential evolution. The encrypted image is decrypted using the same key and all the shares are combined together to get the original image.

REFERENCES

Catley, C., M. Frize, R.C. Walker and D.C. Petriu, 2006. Predicting high-risk preterm birth using artificial neural networks. IEEE. Trans. Inf. Technol. Biomed., 10: 540-549.

Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals, 21: 749-761.

Grangetto, M., E. Magli and G. Olmo, 2006. Multimedia selective encryption by means of randomize darithmetic coding. Trans. Multimedia, 8: 905-917.

Kulkarni, R.V. and G.K. Venayagamoorthy, 2011. Particle swarm optimization in wireless-sensor networks: A brief survey. IEEE. Trans. Syst. Man Cybern. Part C Appl. Rev., IEEE. Trans. Syst 41: 262-267.

Mao, Y. and M. Wu, 2006. A joint signal processing and cryptographic approach to multimedia encryption. IEEE. Trans. Image Process., 15: 2061-2075.

Naor, M. and A. Shamir, 1995. Visual Cryptography. In: Advances in Cryptology, De Santis, A. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-60176-0, pp: 1-12.

Quteishat, A., C.P. Lim and K.S. Tan, 2010. A modified fuzzy min-max neural network with a genetic-algorithm-based rule extractor for pattern classification. IEEE. Trans. Syst. Man Cybern. Part A Hum., 40: 641-650.

Sah, H.R. and G. Gunasekaran, 2014. Privacy preserving collaborative data mining using steganography and encryption. J. Theor. Appl. Inf. Technol., 68: 411-415.

Sah, H.R. and G. Gunasekaran, 2015a. Privacy preserving data mining using image slicing and visual cryptography. Proceedings of the 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT'15), July 13-15, 2015, IEEE, Denton, Texas, Networking Technologies ISBN:978-1-4799-7983-7, pp: 1-7.

Sah, H.R. and G. Gunasekaran, 2015b. Privacy preserving data mining using visual steganography and encryption. Proceedings of the 10th International Conference on Computer Science and Education (ICCSE'15), July 22-24, 2015, IEEE, Cambridge, England, UK., England, ISBN:978-1-4799-6598-4, pp: 154-158.

Sah, H.R. and G. Gunasekaran, 2016. Preserving data privacy with record retrieval using visual cryptography and encryption techniques. Indian J. Sci. Technol., 9: 1-9.

Toreini, E. and M. Mehrnejad, 2011. Clustering data with particle swarm optimization using a new fitness. Proceedings of the 3rd Conference on Data Mining and Optimization (DMO'11), June 28-29, 2011, IEEE, Putrajaya, Malaysia, ISBN:978-1-61284-211-0, pp: 266-270.

Wang, H. and Y. Zhang, 2011. Improvement of discrete particle swarm classification system. Proceedings of the 8th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD'11) Vol. 2, July 26-28, 2011, IEEE, Shanghai, China, ISBN:978-1-61284-180-9, pp: 1027-1031.