OPTIMIZED HYBRID SECURITY MECHANISM FOR IMAGE AUTHENTICATION AND SECRECY USING PSO

K.Kuppusamy[1] and K.Thamodaran[2]

[1,2]Department of Computer Science and Engineering ,
Alagappa University, Karaikudi,
Tamilnadu, India-630003.

ABSTRACT

Authentication is one of the image security issues solved by hash function and another one issue is providing security for illegal manipulation of digital image is solved by an encryption. An optimized hybrid image security mechanism for authentication and secrecy of images by means of Particle Swarm Optimization (PSO) in daubechies4 transform is illustrated in this paper. This mechanism provide solutions to the issues such as authentication, robustness, security and statistical attacks. The PSO technique is employed to select feature vectors to form the image hash and select high energy coefficients for partial encryption. The shuffling of bits , coefficients and blocks of an image is performed by interweaving technique. The Completeness of Signature (CoS) is used to recognize the image as authentic or unauthentic. The image quality distortion is computed with help of image quality index metric(IQIM) with respect to three factors namely loss of correlation, luminance distortion, and contrast distortion. The experimental results are computed with respect to CoS, IQIM, PSNR and correlation coefficient and presented to demonstrate the efficacy of the proposed scheme.

KEYWORDS

Authentication, Confidentiality, dabechies4, encryption, hash function, Interweaving, IQIM, and PSO.

1. INTRODUCTION

The accelerate growth of multimedia applications and the development of internet technology the digital media contents can be transmitted opportunely over networks and it is essential to secure them from leakages. The robust security scheme is essential to store and convey digital images such as important medical images, confidential databases of military image, private video conferencing, secret personal photograph. The requirements to accomplish the security needs of digital images have led to the development of good hashing and encryption techniques. An image hashing techniques are extract a set of features from the image to form a compact representation that can be used for authentication. Hashing techniques are necessary to verify authentication, content integrity and prevent forgery. An authenticity of image is appraised by means of digital signature while the image is affected by incidental distortions. Cryptography is very important to provide secrecy and security against statistical attacks and other types of attacks when swap over images between two parties on the network[18].

In the literature review, different methods of digital image authentication techniques, image encryption techniques and hybrid image security techniques have been reported. Image hashing techniques use data from different domains such as DCT coefficients[5], Wavelet transform

coefficients[19] and Fourier transform coefficients[13], [15], Daubechies wavelet transform[3] to generate the signature for image authentication. A digital signature is an encrypted form of the whole data generated from original data. Chai Wah Wu has proposed an image authentication technique using DCT coefficient relationship in which the DCT coefficients are first scaled and quantized. Then, a binary string is generated which is considered as content hash[5]. Ee-Chien Chang et al. illustrates a content-based spatial domain image authentication scheme. In this scheme an extremely low-bit-rate contents are considered for generating the digital signature. This scheme is robust against image processing distortions like low-pass filtering ,JPEG compression and tampering[7]. Takeyuki Uehara et al. have suggested an image authentication scheme. This scheme constructs a message authentication code integrating a number of feature codes which are protects the region of interest in the image and also tolerates JPEG compression[9]. Sun.Q.et al., have projected an image authentication scheme using EBCOT process and ECC based encryption to generate digital content based signature. The feature extraction is applied after the EBCOT process. This scheme is capable of resisting all distortions during JPEG2000 compression[10].

Nabin Ghoshal et al. have designed an image hashing scheme using Discrete Fourier Transformation for authentication of gray level PGM, TIFF images. The image data are transformed to frequency domain with help of sub matrix of 2x2 size of host image. The MD-5 is used to generate 128 bits Message Digest [13]. H.B.Kekre et al. have illustrated an image hashing scheme using CBIR and hamming distance. The generated hash value is used to pull out the images with respect to query image among large image database [15]. Fawad Ahmed et al. have demonstrated a wavelet-based image hashing scheme using PHF and secret key. This scheme resolves the issues such as security, tamper detection and robustness. The secret key is used randomly modulate image pixels to create a transformed feature space. A 4-bit quantization scheme is employed to decrease the size of the hash [19]. Harsh Kumar Sarohi et al. have presented perceptual hashing scheme for content based image retrieval. In this scheme perceptual hash function is used to generate comparable hash features for related images. In order to match up two perceptual hash features an adequate distance or similarity function is used. An authentication result is decided based on the two perceptual hash features[25]. Kelsey Ramirez-Gutierrez et al. have suggested two perceptual image hashing schemes which includes the features such as geometric alterations, determining potentiality, finding tampered regions. The modifications of these algorithms are analyzed which improve their performance by increasing their robustness against geometric distortions providing them also tamper detection capability [26].

Selective or partial encryption techniques are used to protect only the visually most important parts of an image which reduce the computational difficulties in all applications. H.Cheng et al. have dealt an image encryption scheme in which quad tree algorithm is used to compress the images, and encrypt only the resulted tree structure and leaving the remaining parts unencrypted[2]. S.Lian et al. have proposed a frequency domain selective image encryption scheme using wavelets transform and JPEG2000 lossy compression standard. The selective encryption of significant bit-planes of wavelet coefficients in high and low frequency reduces the encryption data ratio to less than 20% and encryption time ratio deducted to less than 12%. This scheme is tough to various attacks such as plaintext attack and brute-force attack and not to compression ratio [8].

Flayh.N.A. et al. have discussed a partial encryption scheme. This scheme encrypt only important part of the host images of gray scale as well as color images. It is noted that encryption and decryption time are decreased[14]. Shiling Yan et al. have detailed a partial encryption scheme to encrypt JPEG2000 images based on EBCOT. EBCOT codes are classified into five categories,

analyze effects of each type of data on image reconstruction, and then select two types of significant data to encrypt using a stream cipher[20]. Sateesh.S.V.V. et al. have discussed an image encryption scheme using DCT domain and LFSR. In this scheme particular points of DCT transformed image data are encrypted with respect to random number generated by LFSR. In order to increase the throughput of the scheme the optimized algorithm and arithmetic operators are used [22]. N.Tanejaa et al. have proposed an image encryption scheme using selective encryption based on wavelet transform in fractional wavelet domain. In this scheme an Arnold cat map is used to perform very selective encryption of image data through normalized information [23]. K.Kuppusamy and K.Thamodaran have suggested an optimized partial image encryption scheme in which high energy coefficients are selected with help of PSO for encryption in daubechies4 transform. An image quality distortion is assessed with respect to loss of correlation, luminance distortion, and contrast distortion [24].

Panduranga.H.T et al. illustrates a concept of selective image encryption in two different schemes. In former scheme only selected blocks are encrypted and in the subsequent scheme selected blocks are partially encrypted using individual map-image [27]. Parameshachari.B.D.et al. have dealt a partial image encryption scheme in which Fourier transform is used for modifying image blocks. The phase manipulation and encryption of sign bit are employed[28]. Kai Chen et al. have intended a hybrid content-based image authentication scheme based on robust Fridrich's content-based and Sun's semi-fragile crypto-hash based authentication schemes. In former scheme global features are used and in the next scheme local features to locate the modified regions [11]. H.Zang et al. have depicted a hybrid image security scheme using encryption and digital signature.This scheme integrates generalized synchronization and Henon discrete-time chaotic system to perform encryption and generate digital signature [16]. Mehrzad Khaki Jamei1 et al. have suggested an image encryption. This scheme uses chaotic maps and complete binary tree for encryption. In this scheme perfect binary tree is used through which the encryption complexity is enhanced but security level is raised [21]. Jinrong Zhu has projected a modified particle swarm optimization scheme in which inertial factor of each particle is revised with respect to approaching degree between the fitness of itself and the optimal particle [17].
The remaining paper is arranged as follows. Section 2 tenders the information concerning particle swarm optimization techniques. Section 3 illustrates the proposed optimized hybrid image authentication and partial encryption scheme based on daubechies4 transform and PSO. Section 4 offers the formulae to compute the performance through CoS, IQIM, PSNR, correlation coefficient, NPCR and UACI. The section 5 monitor the results of the experiments and analyse the security of the proposed scheme and conclusion of this paper is described in section 6.

2. PARTICLE SWARM OPTIMIZATION

Kennedy and Elberhart have developed an evolutionary computation system is known as PSO[1]. A particle swarm optimization technique is formed based on the replication of the social behaviour of bird flocks [12]. Swarm Intelligence is an inventive distributed intelligent concept to solve optimization problems that initially considered its motivation from herding phenomena in vertebrates.

In PSO scheme, the particle is considered as a bird in the search space to produce a solution. Every particle establish the direction and distance of the next move with respect to velocity and optimized function which decides a fitness function [4]. The scheme tracking the optimal particle at present in the solution space. Each particle attempt to revise its position with respect to ensuing information:

- the distance between the present position and particle best

- the distance between the present position and global best

This revision can be represented by the concept of velocity. The revision of velocity of each agent is performed with help of equation (1) in inertia weight approach (IWA)

$$v_{k+1} = w * v_k + c_1 * r_1 * (p_k - x_k) + c_2 * r_2 * (g_k - x_k) \quad (1)$$

where,w –non negative inertia factor, v_k - velocity of particle , x_k - present position of particle, c_1-determine the relative influence of the cognitive component, c_2- determine the relative influence of the social component, p_k - *pbest* of particle , g_k - *gbest* of the group, r_1, r_2 - the population is getting diversity with help of random numbers and are consistently distributed in the interval [0,1]. The particle make a decision to move to next position by means of equation (1) and regarding its own experience, which is the memory of its best earlier position, and the practice of its most successful particle in the swarm. The particle explores the solution in the problem space in the range of [−s, s]. The particle updating its position by means of equation (2).

$$x_{k+1} = x_k + v_{k+1} \quad (2)$$

3. PROPOSED OPTIMIZED HYBRID IMAGE AUTHENTICATION AND PARTIAL ENCRYPTION SCHEME.

The proposed optimized hybrid image authentication and partial encryption scheme offers authentication and confidentiality for digital images. This proposed hybrid scheme is based on the daubechies4 transform, particle swarm optimization and IQIM. The PSO selects the high energy coefficients to a structure the image hash and SHA-512 function compress image hash as robust 512 bit long. In the process of hash creation, the daubechies4 transformed sub bands LL, LH, HL are considered for creating hash features. Among all sub bands, all coefficients of LL sub band are considered and PSO scheme is used to select high energy coefficients with help of 256 bit secret key in 8 x 8 non-overlapped blocks of LH, HL sub bands for creating hash features. PSO select high energy coefficients from hash attached image to accomplish partial encryption. These high energy coefficients are preferred as applicants for partial encryption which momentously decreases the correlation among image pixels. Then shuffling of bits, coefficients and blocks are performed using interweaving technique. An interweaving technique is employed to achieve shuffling of bits, coefficients and blocks. In order to increase the security the sign bit of the particular low frequency coefficients are encrypted. Cryptographically secured pseudo random number direct the whole encryption process.

This scheme offers tough secrecy of the image when reasonable length secret key is used. An image quality distortion is computed with respect to equation (8) based on three features such as loss of correlation, luminance distortion, and contrast distortion. In this paper, a new conception is used to amend the inertial factor correctly is intended. An inertial factor of every particle is altered with respect to on the point of scale between the suitability of itself and the optimal particle. A particle spot its enhanced fitness value by choosing a smaller amount of inertial weight and a particle spot its poor fitness value by choosing a larger inertial weight. The proposed algorithm using this parameter to explore in huge range and the approximate location of the optimal solution is established rapidly. Also the later iterations yield the accurate result by means of seeks in smaller range.

A random number(*rn)* is exercised to decide the suitable inertia weight and also avoid local optimum and early convergence is put off by means of smaller amount of inertial weight.

Considering a maximization problem, the inertial factors of the particles are restructured regarding to equation (3).

$$w_m = \frac{rn}{pm}\left|\frac{f_{cp} - f_{opc}}{f_{opc}}\right|, \quad if \quad w_m > w_0 \text{ then } w = w_m , \quad if \quad w_0 > w_m \text{ then } w = w_0 \tag{3}$$

where, *rn*-random number, *pm* -Parameter, f_{cp} -fitness of current particle, f_{opc} -optimal particle currently.

PSO training for Image authentication scheme is achieved by means of equation (4).

$$\text{Fitness Function } f(x) = \frac{1}{n}\sum_{i=1}^{n} CoS_i \tag{4}$$

Where CoS means Completeness of Signature.

PSO training for Image encryption scheme is achieved by means of equation (5).

$$f(x) = Q + PSNR + R \tag{5}$$

Where Q-image quality index, PSNR- peak signal-to-noise ratio and R- resistance against attacks.

3.1. Key Generation Procedure

Cryptography based secret keys and sub keys are created using pseudo-random number generator for encryption. Four sequences S_1, S_2, S_3 and S_4 with k_1, k_2, k_3 and k_4 are considered as seed values respectively. Sequence S_1 is used to encrypt the sign-bit of the selected coefficients to diffuse the statistics, S_2 is used to perform pixel permutation and S_3 is used to perform coefficient permutation. The sequence S_4 is created using k_4 as the seed value, which is appointed to achieve block permutation.

3.2. The PSO Algorithm

Step 1: The primary position and velocity of the particles are randomly constructed within predefined ranges.
Step 2: The velocities of all particles are restructured at each iteration with respect to equation(1) where *w* will be revised regarding to equation (3).
Step 3: The positions of all particles are restructured with regard to equation(2). The value of x_k is revised within legitimate limit.
Step 4: If the given condition is satisfied the values of pbest and gbest are updated based on equation(6). if f(p_k) > pbest, then pbest = p_k, if f(g_k) > gbest , then gbest = g_k. (6)
where f(x) is considered as objective function for optimization.
Step 5: The steps 2 to 4 are repeated until the given conditions are satisfied. The algorithm yields the values of gbest and f(gbest).

3.3. The Hash Generation Procedure

Step 1: Daubechies4 transform is employed to revise the host image I into four non-overlapping multi-resolution coefficient sets: LL_1, LH_1, HL_1 and HH_1.
Step 2: Perform Daubechies4 further on LL1 coefficients sets to get four coefficient sets: LL_{12}, LH_{12}, HL_{12} and HH_{12}.
Step 3: Generate the secret key s_k.

Step 4: Hash feature is created with regarding all coefficients of daubechies4 transformed LH_{12}, HL_{12} and HH_{12} coefficient sets and PSO pick the high energy coefficients of LH_1, HL_1 coefficient sets.
Step 5: SHA-512 scheme is employed to compress the image hash as 512 bit length.
Step 6: Created hash bits are combined to form the final hash H.
Step 7: Perform entropy coding and obtain I^*.

3.4. The Encryption Procedure

Step 1: Consider Daubechies4 two level transformed hash attached image for encryption .
Step 2: Generate the secret key S_k.
Step 3: PSO select high energy coefficients with help of given secret key from daubechies4 transformed coefficients sets for encryption. The statistical information is disseminated through encrypting the sign-bit of the selected coefficients are encrypted with the sub-key k_1.
Step 4: An interweaving technique carry out on coefficient bits of specified row or column through sub-key k_2, .
Step 5: An interweaving technique carry out on coefficients of specified row or column through the sub-key k_3.
Step 6: An interweaving technique carry out on blocks of specified row or column through the sub-key k_4.

3.5. The Decryption Procedure

In order to decrypt the encrypted image the decryption procedure is applied which is the reverse of the encryption procedure.

3.6. The Hash Extraction Procedure.

Step 1: Daubechies4 transform is employed to alter the host image I^* to decompose it into four non-overlapping multi-resolution coefficient sets: LL_1, LH_1, HL_1 and HH_1.
Step 2: Perform Daubechies4 further on LL_1 coefficients sets to get four coefficient sets: LL_{12}, LH_{12}, HL_{12} and HH_{12}.
Step 3: Generate the secret key s_k.
Step 4: All coefficients of LH_{12}, HL_{12} and HH12 sub bands and selected high energy coefficients of LH_1, HL_1 sub bands through PSO and secret key are considered for creating hash features.
Step 5: SHA-512 function compress the image hash as 512 bit long.
Step 6: Finally the created hash bits are combined to shape the final hash H*.
Step 7: To authenticate the received image match the created hash H* with the received hash H and evaluate the CoS value. The received image is declared as authentic when CoS value is greater than or equal to 0.75 otherwise unauthentic and specify the tampered block numbers.

4. MEASURES OF PERFORMANCE

4.1. Completeness of Signature (CoS)

The proposed technique produces a PSO based optimized hash code or a digest using user defined key value. The computed optimized hash value is then transmitted to the receiver along side with the compressed image. An optimized hash code is created from the received image and compared with the received hash regarding Completeness of Signature (CoS) which is stated by the equation(7) .

(7)

$$\text{CoS}=\frac{\left(F_m - F_n\right)}{F_t}$$

where F_m denotes the number of feature vectors that match, F_n is the number of feature vectors that do not match and F_t is the total number of feature vectors that are considered for generating the optimized hash code. The received image is declared as authentic when the stated condition is fulfilled otherwise unauthentic.

4.2. Image Quality Index Metric (IQIM)

Zhou Wang, Alan. C. Bovik have proposed a mathematically defined system to compute the universal image quality index (IQIM). An image distortion is quantified by means of universal image quality index derived from the three factors namely loss of correlation, luminance distortion, and contrast distortion. Two images *f* and *g* are represented as matrices of size (*M* x *N)* and their pixel values are $f[i,j]$, $g[i,j]$ where ($0 \geq i > M$, $0 \geq j > N$). The image quality *Q* is evaluated as a product of three components as per equation (8):

$$Q = \frac{\sigma_{fg}}{\sigma_f \sigma_g} * \frac{2\bar{f}\bar{g}}{(\bar{f})^2 + (\bar{g})^2} * \frac{2\sigma_f \sigma_g}{\sigma_f^2 + \sigma_g^2} \tag{8}$$

where

$$\bar{f} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} f[i,j], \qquad \bar{g} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} g[i,j]$$

$$\sigma_{fg} = \frac{1}{M+N+1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f[i,j]-\bar{f})*(g[i,j]-\bar{g})$$

$$\sigma_f^2 = \frac{1}{M+N-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f[i,j]-\bar{f})^2 , \qquad \sigma_g^2 = \frac{1}{M+N-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(g[i,j]-\bar{g})^2$$

The correlation coefficient is evaluated through first component to asses the degree of linear correlation between images *f* and *g* lies in the interval [-1, 1]. When *f* and *g* are linearly related yields the best value 1 which designate that $g[i,j] = a*f[i,j]+b$ for all possible values of *i* and *j*. The luminance is evaluated through second component to asses mean luminance between the images lies in the interval [0, 1]. Because σ_f and σ_g can be treated as compute the contrast of *f* and *g*. Then the contrast is evaluated through third component to measure disparity between the images lies in the interval [0, 1]. An interval for the index *Q* is [-1, 1]. When two images are same the *Q value* is 1. Quality Index Computes the universal image quality index [6]**.**

4.3. Peak Signal-To-Noise Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is employed to determine the quality of partially encrypted image regarding to equation (9).

$$\text{PSNR} = 10 \log_{10}\left(\frac{\text{MAX}^2}{\text{MSE}}\right) \tag{9}$$

where MSE indicates square error.

4.4. Correlation Coefficient

The correlation between adjacent pixels in a ciphered image are analyzed by calculating the correlation coefficients according to the equation (10).

$$r_{xy} = \frac{COV(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \text{where} \quad E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \qquad (10)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \qquad COV(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

The two formulae Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) stated in equations (11) and (12) correspondingly are used to examine the manipulation of one-pixel change on the entire image encrypted by the proposed scheme. For example consider two ciphered-images be denoted by C1 and C2, whose related plain-images have only one pixel variation. The values of the pixels are stored at array (i, j) in C1 and C2 by C1(i, j) and C2(i, j), correspondingly. Construct a 2D array D, with the equal size as images C1 and C2. Then, D(i, j) is established by C1(i,j) and C2(i,j), if C1(i,j) = C2(i,j) then D(i,j) = 1; otherwise, D(i, j) = 0. The NPCR is defined as

$$NPCR = \frac{\sum_{i,j} D(i, J)}{WxH} x\,100 \ \% \qquad (11)$$

where width and height of C1 and C2 are represented by W and H correspondingly and NPCR quantify the percentage of altered pixel numbers between these two images.

$$UACI = \frac{1}{WxH}\left[\sum_{i,j} \frac{C_1(i, j) - C_2(i, j)}{255}\right] x\,100 \ \% \qquad (12)$$

which quantify the average intensity of variations between the two images.

5. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

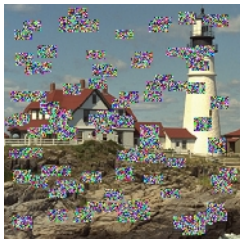
In this proposed system the optimized hybrid image security scheme for authentication and secrecy with daubechies4 and particle swarm optimization is implemented. Visual Studio .NET (C#.Net) is used for implementation and testing the image processing experiments.

The proposed optimized hybrid image security scheme illustrated in section 3 has been experimented through more than 100 different images. The experimental images are of size (512 x 512) with pixel values in the range 0 - 255. For example standard host image namely lighthouse image is considered which is shown in Figure1(a). Only 35% of coefficients are selected for encryption in these experiments. The partially encrypted version of the test image lighthouse is shown in Figure 1(b) Permutation with partially encrypted hash attached test image lighthouse is shown in Figure1(c). The 256 bit secret key is created by means of pseudorandom numbers for choosing high energy coefficients with help of PSO for hash generation and partial encryption. The SHA-1 is utilized to extract hash bits in 512 bit long. In order to create hash features all coefficients of LH_{12}, HL_{12} and HH_{12} sub bands and chosen high energy coefficients of LH_1, HL_1

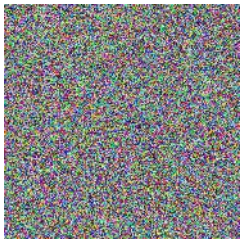
sub bands through PSO and secret key are considered. The sub bands are divided as 8 x 8 non-overlapped blocks. The p = 25, r_1 = 1, r_2 = 1, are defined as parameters for experiments. An interweaving technique is used for shuffling of bits, coefficients and blocks. The performance of the proposed optimized hybrid image security scheme for authentication and secrecy scheme is measured by calculating the CoS, IQIM, PSNR and correlation coefficient.

The correlation between the embedded and extracted hash features of lighthouse image are measured by the metric CoS according to equation(7) as described in Section 4 and is found to be 0.9923 in PSO based system and 0.9804 in without PSO based system which indicates effective authentication. The quality of the hash attached encrypted lighthouse image is assessed with respect to original image by means of IQIM regarding to equation (8) as illustrated in section 4. The IQIM value is identified as to be 0.0026 in PSO based system and 0.0037 in without PSO based system which denotes successful encryption. In addition to that the quality of the hash attached encrypted lighthouse image is assessed with respect to original image by means of PSNR regarding to equation (9). The PSNR value is identified as 8.3624 dB in PSO based system and 9.1593 dB in without PSO based system which also denotes successful encryption. The correlation between the adjacent pixels in a encrypted image are assessed as per equation (10) as illustrated in Section 4. The correlation value is identified as 0.0746 in PSO based system and 0.0853 in without PSO based system which denotes efficient encryption. In order to get the original image the hash attached encrypted image is decrypted through secret key which is shown Figure.1(d). Results are observed and recorded in two groups in names of without PSO and with PSO. The experiment is conducted on different test images and results are integrated in table 1 and table 2. From the experimental results recorded in table 1 and table 2 indicates that the proposed PSO based hybrid scheme gives better results than without PSO.

1.(a)



1.(b)



1.(c)

1.(d)

Figure1.(a)Original Image,
1.(b) Hash attached Partially Encrypted image,
1.(c) Permutation With Partially Encrypted Hash Attached Image,
1.(d) Decrypted Image

Figure1. Encryption and Decryption of Hash Attached Lighthouse Image.

Table 1: Authentication Results after Hash Extraction on Images.

Image	Completeness of Signature(COS)			
	WOPSO		PSO	
	COS	A/UA	COS	A/UA
Couple	0.8225	A	0.8931	A
Lighthouse	0.9804	A	0.9923	A
Mandrill	0.9152	A	0.9364	A
Parrots	0.9576	A	0.9847	A
Pepper	0.8637	A	0.9025	A

A-Authentic, UA-Unauthentic

Table 2: Robustness of the Proposed Hybrid Scheme On IQIM, PSNR And Correlation Vs Without PSO .

Image	IQIM		PSNR		Correlation	
	WOPSO	PSO	WOPSO	PSO	WOPSO	PSO
Couple	0.0064	0.0057	9.2471	8.7006	0.0884	0.0792
Lighthouse	0.0037	0.0026	9.1593	8.3624	0.0853	0.0746
Mandrill	0.0059	0.0048	9.7291	9.3815	0.0982	0.0933
Parrots	0.0078	0.0022	8.9164	8.4423	0.0465	0.0231
Pepper	0.0082	0.0065	9.1593	8.3624	0.0853	0.0746

5.1. Key Space Analysis

With the intention of provide security the key space must be large adequate in an image cryptosystem to secure against brute force attack. The proposed algorithm makes use of a key of length 256 bits and therefore an attacker has to try out 2^{256} ($2^{256} \approx 1.1579 \text{ X } 10^{77}$) combinations of the secret key. For better encryption of an image such a large key space is adequate for stable use.

5.2. Key Sensitivity Analysis

Three little bit altered secret keys are used to test the sensitivity of key. Initially the test image is encrypted through key-1 of 256 bit long and ciphered image shown in Figure2(a). Next LSB one element of key is altered to shape key-2 and is utilized to encrypt the same test image to get the ciphered image and the same is shown in Figure2(b). Likewise MSB one element of key is altered to form key-3 and is utilized to encrypt the same test image to get the ciphered image and the same is shown in Figure2(c). Ultimately the encrypted images through slightly altered keys, are compared. It is monitored that the image shown in Figure 2(a) is varied from the image shown in Figure 2(b) and the disparity image is offered in Figure 2(d). Similarly the image shown in

Figure2 (a) is varied from the image shown in Figure 2(c) and the disparity image is offered in Figure 2(e). It is hard to compare the encrypted images by merely observing these images. From the results of such comparisons the correlation between the related pixels of the three encrypted images is assessed using the formula given in equation (10). The correlation coefficients between the related pixels of the three encrypted images regarding with the aforesaid littlebit altered keys, is offered In Table 3. The derived results indicate that there is no correlation survives between the encrypted images although these images have been created through little bit altered secret keys.

For example, when a secret key-1 is used to encrypt the light house image and a little bit altered key-2 and key-3 attained by changing one element in LSB and MSB of key-1 correspondingly , are utilized to decrypt the encrypted light house image. The results indicates that two decryptions are unsuccessful as shown in Figure2(f) and Figure2(g). To examine the power of one-pixel (100x100) modification on the plain light house image, the NPCR and UACI formulae stated in equations (11) and (12) correspondingly are utilized on encrypted images. The encrypted images are denoted as C1 and C_2 whose related plain images have only one pixel variation. The results attained as NPCR is 0.3894 and UACI is 0.6241 that point out the proposed scheme is competent to rebel different attacks.

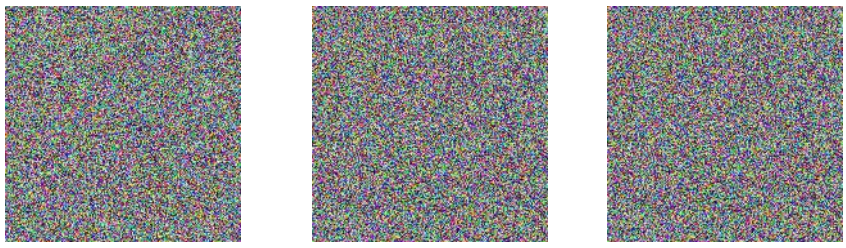


Figure 2.(a) Light house Image Encrypted Using Key-1
Figure 2.(b) Light house Image Encrypted Using Key-2
Figure 2.(c) Light house Image Encrypted Using Key-3

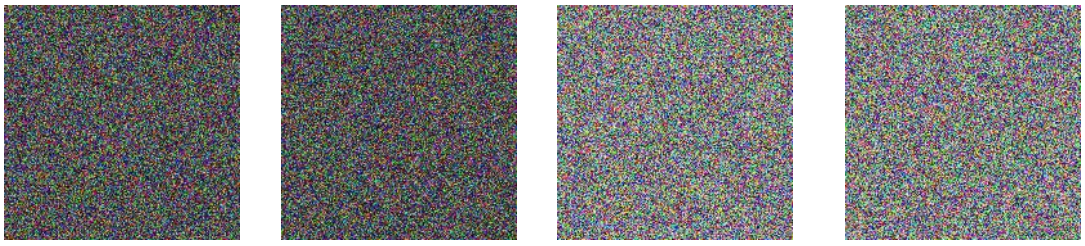


Figure 2(d) Difference Between Fig..2(a) & Fig..2(b)
Figure 2(e) Difference Between Fig..2(a) & Fig..2(c)
Figure 2(f) Unsuccessful Decryption Of Figure 2(a) Using Slightly Modified Key2
Figure 2(g) Unsuccessful Decryption Of Figure 2(a) Using Slightly Modified Key3
Figure 2. Key Sensitivity Test

Table 3. Correlation Coefficients Between the related Pixels of the Two Encrypted Images attained through minor altered Secret Keys On Lighthouse Image

Image1 obtained using key	Image2 obtained using key	Correlation coefficient	
		WOPSO	PSO
Sk1	Sk2	0.0746	-0.0645
Sk1	Sk3	0.0754	-0.0587
Sk2	Sk3	0.0733	-0.0574

5.3. Statistical Analysis

In order to display the resistant power of proposed algorithm to statistical attacks, an experiment is conducted on the histogram of enciphered image. More number of color images of size (512 x 512) are utilized for this plan and their histograms are matched with their related encrypted image. For illustration one instance is shown in Figure (3). The histogram of the original light house image includes large spikes as shown in Figure3(a) although the histogram of the encrypted light house image includes more identical as shown in Figure3(b). It is obvious that the histogram of the encrypted image is noteworthy dissimilar from the relevant histogram of the original image and has no statistical resemblance to the original image. The results indicates that proposed partial image encryption scheme is competent to statistical attacks.

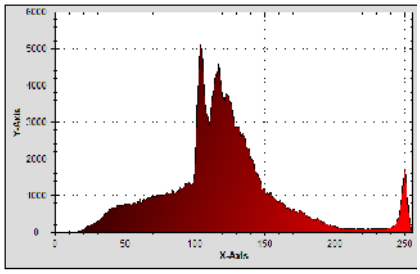


Figure3(a) Original Image

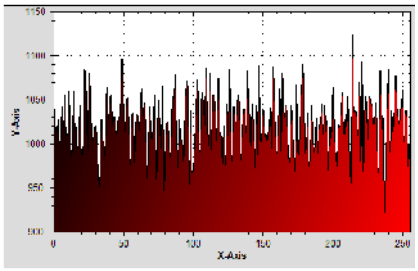


Figure3(b) Encrypted Image

Figure.3. Histograms of Original and Hash Attached Partially Encrypted Lighthouse Image.

6. CONCLUSIONS

An optimized hybrid image authentication and secrecy scheme with daubechies4 and particle swarm optimization has been presented in this paper. In this method, the daubechies4 transform is applied on the cover image. The system selects the high energy coefficients among the daubechies4 based transformed coefficients to generate the hash code and encryption using PSO. Interweaving technique is used to reduce the correlation among the image pixels using the daubechies4 based transformation by making a combination of bit shuffling, coefficient shuffling and block shuffling. Additionally selected coefficients sign bit are encrypted in order to diffuse

statistics. Cryptographically secured keys and sub-keys are created through pseudo-random number to execute encryption. The results of the proposed image security scheme are compared with that without PSO scheme. The experimental results point out that the proposed optimized hybrid authentication and encryption scheme offers very low encryption IQIMs, PSNRs and are resistant to statistical analysis. The proposed security scheme yields the advantage of partial encryption and all the individual permutation scheme. The proposed encryption scheme defends against intruder. The elevation of security can be further enlarged if necessary, by raising the size of the secret key and by raising the number of permutation in each round.

REFERENCES

[1] Kennedy, J., and Eberhart, R.C.,(1995) "Particle Swarm Optimization", Proc. IEEE International Conference on Neural Networks (Perth, Australia), IEEE Service Center, Piscataway, NJ, IV: 1942-1948.

[2] H.Cheng and X. Li,(2000)"Partial Encryption of Compressed Images and Videos", IEEE Transactions on Signal Processing, 48(8), pp. 2439-2451.

[3] Arne Jense and Anders la Cour-Harbo; (2001) "Ripples in Mathematics: the Discrete Wavelet Transform", Springer Publications.

[4] Clerc.M. and Kennedy.J.,(2002) "The particle swarm-explosion, stability, and convergence in a multidimensional complex space", IEEE Transactions on Evolutionary Computation,vol 6(1), pp 58-73.

[5] Chai Wah Wu., (2002) "On the design of content-based multimedia authentication systems", IEEE ransactions on Multimedia, Vol. 4, No. 3, pp385-393.

[6] Zhou Wang, Alan. C. Bovik, (2002) "A universal image quality index", IEEE Signal Processing Letters, vol.9, no.3, pp.81-84.

[7] Ee-Chien Chang, Mohan S. Kankanhalli, Xin Guan, Zhiyong Huang, YinghuiWu, (2003) "Robust image authentication using content based compression.Multimedia Systems", Springer-Verlag, pp1-10.

[8] S. Lian, J. Sun, D. Zhang and Z. Wang, (2004) "A Selective Image Encryption Scheme Based on JPEG2000 Codec", Springer-Verlag, Berlin Heidelberg LNCS 3332, pp.6572.

[9] Takeyuki Uehara, Reihaneh Safavi-Naini and Philip Ogunbona, (2004) "A secure and flexible authentication system for digital images", Multimedia Systems, Springer Verlag, Vol. 9, pp. 441-456.

[10] Sun.Q,Chang.SF., (2005) "A secure and robust digital signature scheme for JPEG 2000 image authentication", IEEE Transcations on Multimedia, vol.7(3), pp 480–494.

[11] Kai Chen, Xinglei Zhu, Zhishou Zhang, (2007) "A Hybrid Content-Based Image Authentication Scheme", Springer-Verlag Berlin Heidelberg LNCS 4810, pp.226–235.

[12] Maurice Clerc, (2007), "Particle Swarm Optimization", ISTE publishers,First South Asian Edition.

[13] Nabin Ghoshal, Jyotsna Kumar Mandal, (2008) "A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier TransformationTechnique", Malaysian Journal of Computer Science, Vol. 21(1), pp24-32.

[14] Flay.N.A., Parveen.R., Ahson,S.I., (2009)"Wavelet based partial image encryption", International Conference on Multimedia", Signal Processing and Communication Technologies, IEEE explore , pp 32 – 35.

[15] H. B. Kekre, Dhirendra Mishra , (2009) "Image Retrieval Using Image Hashing", Techno-Path: Journal Of Science, Engineering & Technology Management, Vol. 1 No.3.

[16] H.Zang, L.Min, Li Cao, (2009) "An Image Encryption and Digital Signature Scheme Based on Generalized Synchronization Theorem", International Conference on Computational Intelligence and Security.

[17] Jinrong Zhu, (2009) "A Modified Particle Swarm Optimization Algorithm" Journal Of Computers, Vol. 4, No.12, pp1231-1236.

[18] Behrouz A.Forouzan, (2010) "Cryptography and Network Security", TMH Edition, 2010.

[19] Fawad Ahmed, M.Y.Siyal, Vali Uddin Abbas, (2010) "A secure and robust hash based scheme for image authentication", Signal Processing, Elsevier, pp 1456–1470.

[20] Shiling Yan, Qiuhua Lin, (2010) "Partial encryption of JPEG2000 images based on EBCOT", International Conference on Intelligent Control and Information Processing , IEEE explore, pp 472 – 476.

[21] Mehrzad Khaki Jamei, Rasul Enayatifar and Hamid Hassanpour,(2011)"Hybrid model of chaotic signal and complete binary tree for image encryption", International Journal of the Physical Sciences Vol. 6(4), pp. 837-842.

[22] Sateesh.S.V.V., Sakthivel.R., Nirosha.K.,Kittur, H.M.,(2011)"An optimized architecture to perform image compression and encryption simultaneously using modified DCT algorithm", International Conference on Signal Processing, Communication, Computing and Networking Technologies, IEEE explore, pp 442 – 447.

[23] N.Tanejaa,B.Ramanb,I.Guptaa,(2011)"Selective image encryption in fractional wavelet domain", Elsevier International Journal of Electronics and Communications, vol 65, pp.338-344.

[24] K.Kuppusamy, K.Thamodaran,(2012)"Optimized Partial Image Encryption Scheme using PSO", IEEE International Conference On Pattern Recognition, Informatics and Medical Engineering, IEEE Explorer, pp 236-241.

[25] Harsh Kumar Sarohi, Farhat Ullah Khan, (2013)" Image Retrieval using Perceptual Hashing", Journal of Computer Engineering, Volume 9, Issue 1, PP 38-40.

[26] Kelsey Ramirez-Gutierrez, Mariko Nakano-Miyatake and Hector Perez-Meana, (2013) "Image authentication using perceptual hashing", Academic Journal Scientific Research and Essays Vol. 8(11), pp. 447-455.

[27] Panduranga. H.T, NaveenKumar.S.K,(2013)" Selective image encryption for Medical and Satellite Images", International Journal of Engineering and Technology , Vol. 5., No 1., pp 115 -121.

[28] Parameshachari B D, K M Sunjiv Soyjaudah,Sumitrha Devi K A,(2013) "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications, Vol. 63,No.16.

AUTHORS

Dr.K.KUPPUSAMY is working as Professor in the Department of Computer Science and Engineering, Alagappa University, Karaikukdi, Tamilnadu, India. He has received his Ph.D in Computer Science and Engineering from Alagappa University, Karaikudi, Tamilnadu. He is having rich teaching P.G. experience about 27 years in ever growing Computer Science field. He is guiding more Mphil., and P.hD., scholars. He has Presented many research papers in the National and International conferences and published many research papers in National and International Journals. His areas of research interest includes Information/Network Security, Algorithms, Neural Networks, Fault Tolerant Computing, Software Engineering and Testing and Optimization Techniques.

K.THAMODARAN is a research scholar in the Department of CSE, Alagappa University, Karaikukdi, Tamilnadu, India. He has received his M.Sc(CS) degree and M.Phill(CS) degree from Bharathidasan University, Trichy, TamilNadu, India. He is having teaching experience around 21 years. He has published 4 research papers in International Journals and presented 6 papers in the National and International conferences. His area of interest includes Network Security, Image Security and Optimization Techniques.