OPTIMIZED HYBRID IMAGE SECURITY SCHEME FOR COPYRIGHT PROTECTION, AUTHENTICATION AND CONFIDENTIALITY USING PSO

K. Kuppusamy

Professor, Dept. of Computer Science and Engineering , Alagappa University, India

K. Thamodaran

Research Scholar, Dept. of Computer Science and Engineering , Alagappa University , India

Abstract

The digital watermarking scheme provides copyright protection, the hash function provides an authentication, and an encryption scheme provides security against illegal duplication and manipulation of multimedia contents especially to digital images. In this paper an optimized hybrid image security scheme for copyright protection, authentication and security of digital images using Particle Swarm Optimization(PSO) in daubechies4 wavelet transform is proposed. This scheme provide solutions to the issues such as copyright protection, authentication, robustness, security, statistical attacks and confidentiality. The coefficients are selected in daubechies4 domain with help of PSO to embed the DCT transformed selected high energy coefficients watermark bits in the host image. The features are extracted in daubechies4 domain with help of particle swarm optimization(PSO) to generate the image hash. The selected coefficients are encrypted in Daubechies4 domain with help of PSO. The image quality index metrics (IQIM) is used to measure the image quality distortion. The experimental results are evaluated with respect to BCR, CoS, IQIM, PSNR,and correlation and presented to demonstrate the competence of the proposed scheme.

Keywords: Dabechies4, fitness function, IQIM, interweaving, PSO, security

Introduction

A recent propagation and accomplishment of the Internet, together with availability of conomical digital storage devices and tools has created a platform to duplicate , distribute and tamper the digital contents easily. Thus the protection of the intellectual property rights, authentication and confidentiality of digital images becomes an important issue. The

watermark is an owner designed logo or trademark, which can be hidden in the owner's image products. Hashing techniques are essential to the verify authentication, content integrity and prevent forgery. The digital signature is used to validate correctly when the image is incidentally damaged such as compression and filters. cryptography is very important to provide confidentiality and security against statistical attacks and other types of attacks when exchange images between two parties on the network [Bruce Schneier,1996]. Arne Jense and Anders la Cour-Harbo explained the features of daubechies4 transform(Arne Jense et al,2001).Latha Parameswaran et al. have proposed the content-based image watermarking scheme for authentication in which, hybrid of Independent Component Analysis(ICA) and DCT is used. ICA is applied to each block of divided host image and the mixing matrix of the block is determined[Latha Parameswaran et al.,2008].

Chih-Ming Kung et al. have proposed the image watermarking scheme using frequency domain and signature process. It uses the self-information of coefficients of the middle frequency in the host image, and explicitly takes in the cross-correlation between the coefficients of middle frequency and the watermark[Chih-Ming Kung et al.,2009]. Muhammad Ishtiaq et al., have proposed the image watermarking scheme in which the strength selection is performed using an efficient Particle Swarm Optimization(PSO). The watermarking is performed in the DCT domain on the selected mid-band coefficients[Muhammad Ishtiaq et al.,2010].Farhad Rahimi et al.have proposed the image watermarking scheme in which an adaptive dual and oblivious(blind) watermarking scheme is employed in the contourlet domain. Region of interest(ROI) is very important in interpretation by medical doctors rather than region of non-interest[Farhad Rahimi et al.2011].

Parthiban.V. et al. have proposed the image watermarking scheme in which the robustness is improved through combination of DWT and SVD.Linear flexibility of images in terms of scalability, resolution and distortion are achieved by decomposition of images into sub bands using DWT[Parthiban.V.et al.2012].Chai Wah Wu has proposed a hash based authentication scheme using DCT coefficient relationship. In this scheme the DCT coefficients are first scaled and quantized then a binary string is generated which serves as the content hash[Chai Wah Wu, 2002].Takeyuki Uehara et al. have proposed a JPEG-tolerant image authentication scheme which constructs a Message Authentication Code incorporating a number of feature codes that are used to protect regions of interest in the image[Takeyuki Uehara et al.,2004].Ashwin Swaminathan et al. have proposed a scheme for generating an image hash based on Fourier-Mellin transform features which are invariant to two-

dimensional affine transformations and incorporates key-dependent outputs to form a secure and robust image hash[Ashwin Swaminathan et al. 2006].Dittmann.Jet al. have proposed an image encryption scheme which uses selective encryption scheme with extremely low encryption demand focused on to lossless encoded imagery based on the hierarchical progressive coding mode of JBIG [Dittmann.J. et al.2005].Panduranga.H.T et al. Naveen Kumar S.K. have proposed a hybrid image encryption scheme based on the concept of carrier image and SCAN patterns generated by SCAN methodology[Panduranga.H.T et al.,2010].

Mehrzad Khaki Jamei et al. have proposed a image encryption scheme using chaotic signals and complete binary tree. In this scheme higher security is achieved by changing the amount of gray scale of each pixel of the original image[Mehrzad Khaki Jamei et al.,2011]. Xiaoyi Zhou et al. have proposed a hybrid-key based image encryption scheme and authentication scheme. Ergodic matrices are used as public keys in the encryption and decryption process and also as used as essential parameters in the confusion and diffusion stages[Xiaoyi Zhou et al. 2011].Rakesh.S et al. have proposed a hybrid scheme for watermarking and encryption of images using contourlet transform and singular value decomposition[Rakesh.S et al. ,2012].Federica Battisti et al. have proposed a hybrid scheme for watermarking and encryption of images using key-dependent wavelet transform domain and Fibonacci-Haar transform[Federica Battisti et al.,2009].Jinrong Zhu has proposed a modified particle swarm optimization algorithm inwhich every particle chooses its inertial factor according to the approaching degree between the fitness of itself and the optimal particle[Jinrong Zhu,2009].K.Kuppusamy et al. have proposed an optimized partial image encryption scheme, inwhich high energy coefficients are selected with help of particle swarm optimization for encryption in daubechies4 transform. The universal image quality index *Q* is calculated to measure the image quality distortion[K.Kuppusamy et al.,2012]. K.Kuppusamy et al. have proposed optimized digital watermarking scheme, in which the watermark is embedded in the daubechies4 transform domain based on PSO and IQIM are proposed.Then, the DCT transformed selected watermark bits are embedded in the selected coefficients of image[K.Kuppusamy et al. ,2012].In this paper an optimized hybrid image security scheme for copyright protection, authentication and security of images using Particle Swarm Optimization(PSO) and daubechies4 transform is proposed. The results of experimentation on the robustness of the proposed scheme to unintentional manipulations like lossy compression, noise and sensitivity to intentional attacks like insertions, crop, rotations are also presented in this paper.

The rest of this paper is organized as follows. The next section provides the information about particle swarm optimization techniques. The third section describes the proposed optimized hybrid digital image watermarking, authentication and partial encryption scheme based on daubechies4 transform and PSO. The formulae for measure of performance like to BCR, CoS, IQIM, PSNR, correlation coefficient, NPCR, and UACI are given in fourth section.The experimental results and security analysis are presented in fifth section and final section concludes this paper.

Particle Swarm Optimization

Kennedy et al. have constructed an evolutionary computation model known as PSO[Kennedy et al.,1995]. A particle swarm optimizer is a population-based stochastic optimization algorithm modelled after the simulation of the social behaviour of bird flocks[Maurice Clerc,2007]. Swarm Intelligence is an inventive distributed intelligent paradigm for solving optimization problems that originally took its inspiration from the biological examples by swarming, flocking and herding phenomena in vertebrates[Clerc.M .et al.2002]. In PSO algorithm, every solution of the optimization problem is regarded as a bird in the search space, which is called particle. Every particle has a velocity by which the direction and distance of the flying of the particle are determined, and a fitness that is decided by the optimized function. The particles search in the solution space by pursuing the optimal particle currently. Each particle tries to revise its position using the following information:

- the distance between the current position and pbest
- the distance between the current position and gbest

This modification can be represented by the concept of velocity. Velocity of each agent can be modified according to the 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 - current 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 - random numbers which are used to maintain the diversity of the population, and are uniformly distributed in the interval [0,1].From equation (1), a particle decides where to move next, considering its own experience, which is the memory of its best past position, and the experience of its most successful particle in the swarm. In the particle swarm model, the

particle searches the solutions in the problem space with a range [−s, s].Every particle updates its position according to the equation (2).

$$x_{k+1} = x_k + v_{k+1} \tag{2}$$

Proposed Optimized Hybrid image watermarking, Authentication and Partial Encryption Scheme using PSO

The proposed optimized hybrid image watermarking, authentication and partial encryption scheme provides copyright protection, authentication and confidentiality for digital images. This proposed hybrid scheme is based on the daubechies4 transform, PSO and IQIM. The 256 bit secret key is used to select high energy coefficients as candidates with help of PSO to embed watermark, generate hash features and partial encryption in daubechies4 transform. The DCT transformed selected high energy watermark bits of watermark are embedded in the host image. Watermarked daubechies transform outputs to form secure and robust 512 bit image hash using SHA-1. In hash generation, the daubechies4 transformed sub bands LL, LH, HL are considered for generating hash features. According to LL all coefficients are considered for feature generation. The high energy coefficients are selected to generate hash features from 8x8 non-overlapped blocks of LH, HL sub bands. High energy coefficients are selected in Hybrid watermarked and hash attached image with help of PSO for encryption. These high energy coefficients are selected as candidates for encryption which significantly reduces the correlation among image pixels. Then shuffling of bits, coefficients and blocks are performed using Interweaving and Iteration method. In addition, the sign bits of the selected low frequency coefficients are encrypted. A symmetric key based cryptographically secure pseudo random process controls the entire encryption process. This method gives strong cipher of the image, whose key length is significantly large. The universal image quality index *Q* is calculated according to equation (8) to measure the image quality distortion based on three factors such as loss of correlation, luminance distortion, and contrast distortion.

A new idea is used to revise the inertial factor suitably is proposed in this paper. The inertial factor of each particle is gained according to approaching degree between the fitness of itself and the optimal particle. A particle identifies its finer fitness value by selecting a lesser inertial weight and a particle identifies its poorer fitness value by selecting a larger inertial weight. The proposed algorithm using this policy to search in large range and the estimated location of the optimal solution is established rapidly and search in small range in the late iterations in order that the exact solution is found. The inertia weight is calculated using a random number(*rn)* in the algorithm in order to jump out from local optimum and a

least inertial weight factor is used to prevent the premature convergence. The inertial factors of the particles are updated according to equation (3).

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

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

Fitness function $f(x)$ for PSO training for watermarking is given in equation (4).

$$f(x) = Q + PSNR + \frac{1}{n}\sum_{i=1}^{n} \lambda_i \; R_i \qquad (4)$$

where, Q-Image Quality Index, PSNR- Peak Signal-to-Noise Ratio,R-resistance against attacks,and weighting factor λ is used to balance the imperceptibility and robustness of the embedded watermark.

Fitness function $f(x)$ for PSO training for Image authentication is given in equation (5).

$$f(x) = \frac{1}{n}\sum_{i=1}^{n} CoS_i \qquad (5)$$

where CoS means Completeness of Signature.

Fitness function $f(x)$ for PSO training for encryption is given in equation (6).

$$f(x) = Q + PSNR + R \qquad (6)$$

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

Proposed Key Generation Procedure

Cryptographically protected keys and sub keys are produced using pseudo-random number generator for watermarking, hash function and encryption. Four sequences S_1, S_2 , S_3 and S_4 with k_1, k_2 , k_3 and k_4 as seed values respectively. In order to diffuse statistics the sign-bit of the selected coefficients are encrypted using the sequence S_1, S_2 used for pixel permutation and S_3 is used for coefficient permutation. The sequence S_4 is generated using k_4 as the seed value is split into two subsequences S_{41} and S_{42} and are employed in block selection and block permutation.

PSO Algorithm

Step 1: The initial position and velocity of the particles are randomly generated within predefined ranges.

Step 2: On each iteration, the velocities of all particles are modified according to equation(1) where inertial factor w will be obtained according to equation (3).

Step 3: The positions of all particles are modified according to equation(2). After updating, x_k should be checked and limited to the allowed range.

Step 4: Update pbest and gbest when condition is satisfied.

if f(p_k) > pbest, then pbest = p_k ,

if f(g_k) > gbest , then gbest = g_k .

where f(x) is the objective function to be optimized.

Step 5: The algorithm repeats steps 2 to 4 until specific terminating conditions are fulfilled, such as a pre-defined number of iterations. The algorithm reports the values of gbest and f(gbest) as its solution.

Watermark Embedding Procedure

The watermark embedding procedure for Daubechies4 domain and PSO is as follows:

Step 1: Perform Daubechies4 on the host image to decompose it into four non-overlapping multi-resolution coefficient sets: LL1, HL1, LH1 and HH1.

Step 2: Perform Daubechies4 again on LL1 coefficients sets to get four coefficient sets: LL12, LH12, HL12 and HH12.

Step 3: Select high energy coefficients in daubechies4 domain with help of particle swarm optimization for embedding watermark bits.

Step 4: Perform DCT on watermark logo. Select high energy coefficients among DCT transformed watermark bits.

Step 5: Generate two uncorrelated pseudorandom sequences by a key. One sequence is used to embed the watermark bit 0 (PN_0) and the other sequence is used to embed the watermark bit 1 (PN_1).

Step 6: Embed the two pseudorandom sequences, PN_0 and P N_1, with a gain factor λ in the the selected coefficient sets of the daubechies4 transformed blocks of host image instead of embedding in all coefficients. If we denote X as the matrix of the high energy coefficient sets, then embedding is performed according to equation (7) .

$$X' = \begin{cases} X + \lambda * PN0 & \text{Watermark\_bit} = 0 \\ X + \lambda * PN1 & \text{Watermark\_bit} = 1 \end{cases} \quad (7)$$

The Hash Generation Procedure

Step 1: Generate the secret key s_k.

Step 2: Form feature vectors using all coefficients of daubechies4 transformed LH12, HL12 and HH12 coefficient sets and select high energy coefficients of LH1, HL1 coefficient sets with help of PSO.

Step 3: Compress the feature vector in required length using SHA-512.

Step 4: Concatenate the hash bits generated to form the final hash H.

Step 5: Perform entropy coding and obtain I^*.

The Encryption Procedure

Step 1: Consider Daubechies4 two level transformed watermarked hash attached image for encryption .

Step 2: Generate the secret key S_k.

Step 3: Select high energy coefficients from daubechies4 transformed coefficients sets for encryption with help of PSO using the given secret key . In order to diffuse statistics the sign-bit of the selected coefficients are encrypted using the sub-key k_1.

Step 4: Select the coefficient bits for interweaving with help of the sub-key k_2, .

Step 5: Select the coefficients for interweaving with help of the sub-key k_3.

Step 6: The sequence S_4 generated using k_4 as the seed value is split into two subsequences S_{41} and S_{42} and are engaged in block selection and block permutation.

The Decryption Procedure

The decryption process is the reverse of the encryption process.

The Hash Extraction Procedure

Step 1: Perform Daubechies4 on the host image I^* to decompose it into four non-overlapping multi-resolution coefficient sets: LL1, LH1, HL1 and HH1.

Step 2: Perform Daubechies4 again on LL1 coefficients sets to get four coefficient sets: LL12, LH12, HL12 and HH12.

Step 3: Generate the secret key sk.

Step 4: Form feature vectors using all coefficients of daubechies4 transformed LH12, HL12 and HH12 coefficient sets and select high energy coefficients of LH1, HL1 coefficient sets with help of PSO.

Step 5: Compress the feature vector in required length using SHA-512..

Step 6: Concatenate the has bits generated to form the final hash H*.

Step 7: Compare the generated hash H* with the received hash H and compute the CoS value. If the CoS value >= 0.75, then declare the image to be authentic else declare the image to be unauthentic and return the tampered block numbers.

Watermark Extraction Procedure

The watermark extracting procedure is the reverse of watermark embedding procedure.

Measures of Performance

Correlation Coefficient

The correlation between the embedded and extracted watermarks measured by bit correct rate (BCR) according to equation (8).The BCR is used to assess the robustness of the watermarking algorithm against different types of digital signal processing attacks.

$$BCR = \left[1 - \frac{1}{Mw \times Nw} \sum_{i=1}^{Mw} \sum_{j=1}^{Nw} [W(i,j) \oplus W'(i,j)]\right] \quad (8)$$

where W and W' are embedded and extracted watermarks respectively, with size of $M_W \times N_W$ and $\oplus$ denotes the exclusive-or (XOR) operation. The larger value of BCR is gives the better result.

Completeness of Signature (CoS)

At the receiver, the optimized hash code is computed on the received image after decompressing and compared against the received hash using a metric called Completeness of Signature (CoS) according to equation (9).

$$\text{CoS} = \frac{(F_m - F_n)}{F_t} \quad (9)$$

where, F_{m}- number of feature vectors that match,F_n - number of feature vectors that do not match and F_t - total number of feature vectors for generating the optimized hash code.

If the CoS value tends to unity the image is declared to be authentic otherwise the image is declared to be unauthentic.

Image Quality Index Metrix (IQIM)

The image quality distortion is appraised with help of universal image quality index (IQIM),which is mathematically defined and suggested by Zhou Wang et al.The image quality distortion is appraised based on the representing the image distortion relative to the reference image as a combination of three factors: loss of correlation, luminance distortion, and contrast distortion. If two images *f* and *g* are considered as a matrices with *M* column and *N* rows containing pixel values *f*[*i*,*j*], *g*[*i*,*j*], respectively ($0 \geq i > M$, $0 \geq j > N$), the universal image quality index *Q* may be appraised as a product of three components:

$$Q = \frac{\sigma_{fg}}{\sigma_f \sigma_g} * \frac{2\bar{f}\bar{g}}{(\bar{f})^2 + (\bar{g})^2} * \frac{2\sigma_f \sigma_g}{\sigma_f^2 + \sigma_g^2} \quad (10)$$

Where

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

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

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

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

The primary component is the correlation coefficient, which appraises the degree of linear correlation between images *f* and *g*. It varies in the range [-1, 1]. The best value 1 is attained when *f* and *g* are linearly related, which means that $g[i,j] = a*f[i,j]+b$ for all possible values of *i* and *j*. The next component, with a value range of [0, 1], appraises how close the mean luminance is between images. Since σ_f and σ_g can be considered as estimates of the contrast of *f* and *g*, the last component appraises how similar the contrasts of the images are. The value range for this component is also[0, 1]. The range of values for the index *Q* is [-1, 1]. The best value 1 is attained if and only if the images are identical. Quality Index appraises the universal image quality index[Zhou Wang et al.2002].

Peak Signal-to-Noise Ratio (PSNR)

The performance of the proposed partial encryption scheme in daubechies4 based transform domain is measured by peak signal-to-noise ratio (PSNR) according to equation(11).

$$PSNR = 10\log_{10}\left[\frac{MAX^2}{MSE}\right] \quad \text{where} \quad MSE = \left[\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[X(i,j)-X'(i,j)\right]^2\right] \tag{11}$$

where *X* and *X'* are the original and the modified images respectively with image size of $M \times N$. The lower values of PSNR yields the better results in encrypted images.

Correlation Coefficient

The correlation between the adjacent pixels in a ciphered image are calculated and analyzed according to equation (12).

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad , \quad COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{12}$$

To examine the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures are used Number of Pixels Change Rate (NPCR)

and Unified Average Changing Intensity (UACI). NPCR and UACI are calculated according to equation (13) and (14) respectively. Let two ciphered-images, whose corresponding plain-images have only one pixel difference, be denoted by C1 and C2. Label the values of the pixels at array (i, j) in C1 and C2 by C1(i, j) and C2(i, j), respectively. Define a bipolar array, D, with the same size as images C1 and C2. Then, D(i; j) is determined by C1(i,j) and C2(i,j), namely, if C1(i,j) = C2(i,j) then D(i,j) = 1; otherwise, D(i, j) = 0. The NPCR is defined as

$$NPCR = \frac{\sum_{i,j} D(i,J)}{WxH} x100\% \quad (13)$$

where W and H are the width and height of C1 and C2, and NPCR measures the percentage of different pixel numbers between these two images.

$$UACI = \frac{1}{WxH}\left[\sum_{i,j}\frac{C_1(i,j) - C_2(i,j)}{255}\right] x100\% \quad (14)$$

which measures the average intensity of differences between the two images.

Experimental Results and Security Analysis

The proposed system optimized hybrid image security scheme for watermarking, authentication and confidentiality with daubechies4 and PSO is implemented in Visual Studio .NET (C#.Net)and is used for implementation and testing the image processing experiments. The proposed scheme explained in section 3 has been experimented with more than 100 different images .The test images are of size (512 x 512) with pixel values in the range 0 - 255. Different watermark logos, all of size (128 x 128) are used.

The high energy coefficients are selected with help of PSO in daubchiese4 transformed domain for watermark embedding, extract hash bits with SHA-1 and partial encryption. Pseudorandom numbers are used to generate 256bit secret key which is integrated to select high energy coefficients. PSO based daubechies4 transformed selected coefficients have large energies so that the embedded watermarks tend to be robust against different kinds of attacks. Then two uncorrelated pseudorandom noise (PN) sequences are generated which represent the ‘0’ and ‘1’ bits of the watermark to be embedded. The PN sequences corresponding to the DCT transformed watermark bits are embedded into the transformed coefficients of the cover image using the embedding function given in equation(7) as described in Section 3.In hash generation process, daubechies4 transformed sub bands LL, LH, HL are considered for generating hash features. According to LL all coefficients are considered for feature generation and PSO is used to select high energy coefficients to generate hash features from 8x8 non-overlapped blocks of LH, HL sub

bands. The Interweaving and Iteration method is used for shuffling of bits, coefficients and blocks.In partial encryption process, the Interweaving and Iteration method is used for shuffling of bits, coefficients and blocks. The parameters p = 20, r_1 = 1, r_2 = 1, are used. In these experiments only 35% of coefficients are selected for encryption.

The lena image (Figure 1(a)) is the cover image and the watermark image is "system" **(**Figure 1(b)), the corresponding watermarked hash attached partially encrypted image is shown in Figure 1(c),Permutation with watermarked hash attached partially encrypted test image lena is shown in Fig. 1(d), decrypted version of the test image lena is shown in Fig.1(e) and the extracted watermark is shown in Fig.1.(f) resultant images of proposed scheme are given in figures(2) and (3).The correlation between the embedded and extracted watermark is measured by the metric BCR according to equation(8) as described in Section 4 and is found to be 0.9963 in PSO based system and 0.9241 in without PSO based system which also signifies effective copyright protection. The correlation between the embedded and extracted hash features of lena image are measured by the metric CoS according to equation(9) as described in Section 4 and is found to be 0.9726 in PSO based system 0.9686 in without PSO based system which signifies effective authentication. The (CoS >= 0.75) then the received image is authentic, otherwise unauthentic.

The image quality index metrix (IQIM) between the original and the watermarked hash attached encrypted lena images is computed according to equation (10) as described in Section 4 and is found to be -0.0029 in PSO based system and -0.0074 in without PSO based system which also signifies effective encryption.The Peak Signal-to-Noise Ratio (PSNR) between the original and the watermarked hash attached encrypted lena images is computed according to equation(11) as described in Section 4 and is found to be 8.1108 dB in PSO based system and 8.4597 dB in without PSO based system which signifies effective encryption. The correlation between the adjacent pixels in a ciphered image are computed according to equation (12) as described in Section 4 and is found to be 0.0752 in PSO based system and 0.0871 in without PSO based system which also signifies effective encryption.The watermarked hash attached encrypted image is then decrypted using the symmetric secret key to get the watermarked hash attached image and is shown Fig.1(e).Results are presented for two categories, namely without PSO and with PSO. The experiment is conducted on test image Lighthouse and is repeated using different cover images and results are incorporated in table 1, table 2, table 3 and table 4. From table 1, table 2, table 3 and table 4 it is evident that the proposed PSO based hybrid scheme outperforms without PSO.

Fig1.(a) Lena Original, **Fig1.(b)** Watermark logo, **Fig.1.(c)**Watermarked Hash attached Partially Encrypted Lena image.

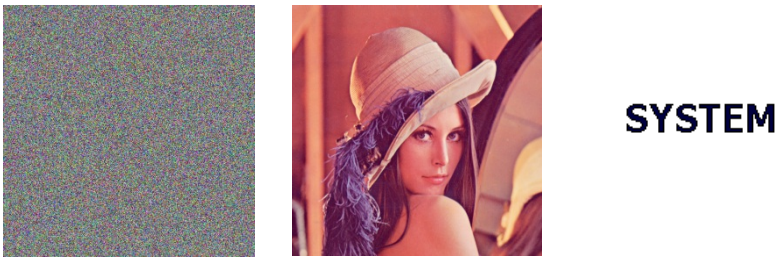


Fig 1.(d) Permutation With Watermarked Hash Attached Partially Encrypted Image , **Fig 1.(e)** Decrypted Image , **Fig.1.(f)** Extracted Watermark.

Fig.1. Encryption And Decryption Of Watermarked Hash Attached Lena Image

Table 1: Results Obtained on correlation between the embedded and the extracted watermarks.

Image	Correlation (BCR)	
	WOPSO	PSO
Lena	0.9241	0.9963
Couple	0.9617	0.9992
Flight	0.9309	0.9817
Sailboat	0.9245	0.9948

Table 2: Results Obtained After Hash Extraction On watermarked Hash Attached Lena And Other Images.

Image	Completeness of Signature(CoS)			
	WOPSO		PSO	
	COS	A/UA	COS	A/UA
Lena	0.9686	A	0.9726	A
Couple	0.8152	A	0.9364	A
Flight	0.8637	A	0.9025	A
Sailboat	0.8225	A	0.8931	A

A-Authentic , UA-Unauthentic

Table 3: Results Obtained After Partial Encryption On IQIM, PSNR And Correlation Values With The Proposed Hybrid Scheme With And Without PSO On Lena And Other Images.

Image	IQIM		PSNR		Correlation	
	WOPSO	PSO	WOPSO	PSO	WOPSO	PSO
Lena	-0.0074	-0.0029	8.4597	8.1108	0.0871	0.0752
Couple	-0.0051	-0.0047	9.0214	8.5706	0.0904	0.0839
Flight	-0.0068	-0.0056	8.4703	8.0261	0.0861	0.0748
Sailboat	-0.0084	-0.0069	8.2534	7.8419	0.0955	0.0891

Key Space Analysis

With the objective of providing security the key space must be large enough in an image cryptosystem to secure against brute force attack. A 256 bits length key is used in this proposed scheme and therefore an attacker has to try out 2^{256} ($2^{256} \approx 1.1579 \text{ X } 10^{77}$) combinations of the secret key. An image cipher with such a large key space is sufficient for stable use.

Key Sensitivity Analysis

With the objective of testing the sensitivity of key ,first encrypt the test image using the 256 bit (key-1) to get the encrypted image shown in Fig. 2(a). Then LSB one element of key is changed to form another key (key-2) and is used to encrypt the same test image to get the encrypted image and the same is shown in Fig.2(b). Similarly MSB one element of key is changed to form other key (key-3) and is used to encrypt the same test image to get the encrypted image and the same is shown in Fig. 2(c).Lastly the images encrypted using the slightly different keys, are compared. It is observed that the image shown in Fig.2(a) is differed from the image shown in Fig. 2(b) and the difference image is presented in Fig. 2(d). Similarly the image shown in Fig.2(a) is differed from the image shown in Fig. 2(c) and the difference image is shown in Fig. 2(e). It is hard to compare the encrypted images by simply observing these images. So for comparison, the correlation between the corresponding pixels of the three encrypted images is calculated using the formula given in Equation (12).

It is perceptible from the results that no correlation exists between the encrypted images even though these have been produced by using slightly different secret keys. Furthermore, when a secret key-1 is used to encrypt an image and a slightly modified key-2 and key-3 obtained by changing one element of key-1 , are used to decrypt the ciphered image, both decryptions are unsuccessful as shown in Fig. 2(f) and Fig. 2(g). To test the influence of one-pixel (100x100) change on the plain image, encrypted by the proposed scheme, two common measures NPCR and UACI according to equations (13) and (14) respectively. Here C1 and C2 are the encrypted images whose corresponding plain images have only one pixel difference. The NPCR and UACI values obtained are 0.2465 and 0.1435 respectively which indicates that the proposed algorithm has reasonably good capability to resist differential attacks.

In Table 4, the correlation coefficients between the corresponding pixels of the three images encrypted using the aforesaid slightly modified different keys, is presented. It is noticeable from the table 4 that no correlation exists among three encrypted images although these have been created using slightly different secret keys.

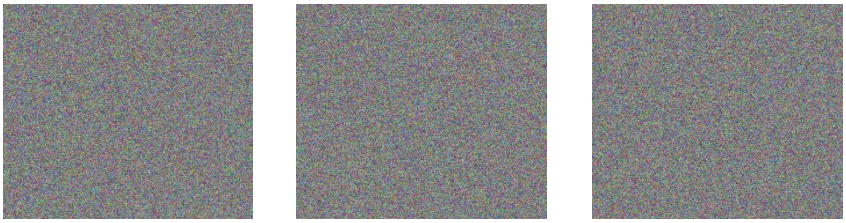


Fig.2.(A) Test Image Encrypted Using Key-1. **2.(B)** Test Image Encrypted Using Key-2. **2.(C)** Test Image Encrypted Using Key-3.

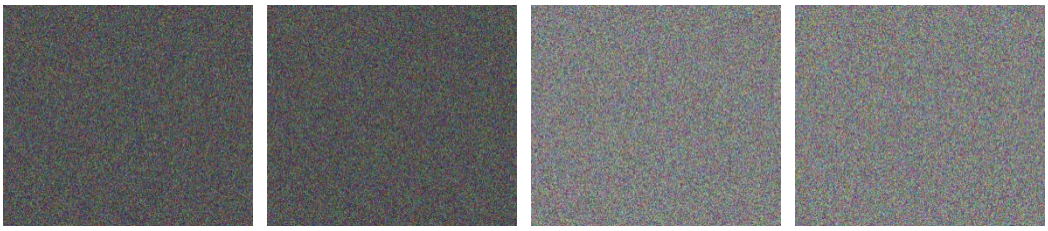


Fig.2.(D) Difference Between Fig..2(A) & Fig..2(B) , **2 (E)** Difference Between Fig..2(A) & Fig..2(C).Fig.2. **(F)** Unsuccessful Decryption Of Fig 2(A) Using Slightly Modified Key2,Fig.2. **(G)**Unsuccessful Decryption Of Fig. 2(A) Using Slightly Modified Key3.

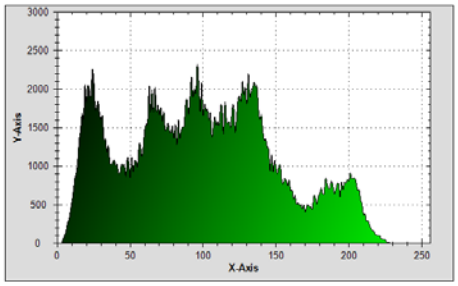
Fig.2. Key Sensitivity Test

Table 4. Co rrelation Coefficients Between The Corresponding Pixels Of The Two Encrypted Images Obtained By Using Slightly Different Secret Keys On Lena Image

Image1 obtained using key	Image2 obtained using key	Correlation coefficient	
		WOPSO	PSO
Sk1	Sk2	0.0751	0.0736
Sk1	Sk3	0.0765	0.0751
Sk2	Sk3	0.0750	0.0747

Statistical Analysis

To demonstrate that the proposed algorithm has dominant resistance to statistical attacks, test is carried out on the histogram of enciphered image. Several color images of size (512 x 512) are selected for this purpose and their histograms are compared with their corresponding ciphered image. One typical example is shown in Fig.(3). The histogram of the plain image contains large spikes as shown in Fig. 3(a) but the histogram of the cipher image as shown in Fig. 3(b), is more uniform. It is clear that the histogram of the encrypted image is, significantly different from the respective histogram of the original image and bears no statistical resemblance to the plain image. Hence statistical attack on the proposed image encryption scheme is very hard.



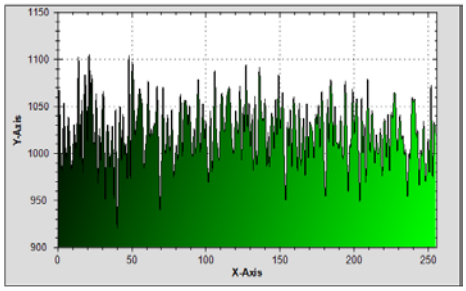


Fig.3 (A) Original Image **Fig.3 (B)** Encrypted Image

Fig.3. Histograms Of Original And watermarked Hash Attached Partially Encrypted Lena Image.

Conclusion

The proposed optimized hybrid image security scheme with daubechies4 and PSO is experimented on different images and is compared with without PSO. The system selects the high energy coefficients among the daubechies4 based transformed coefficients to embed watermark, to generate the hash code and for partial encryption using PSO. The achieved image quality is found to be better in the case of the PSO based watermarking, hash function and encryption. Since the technique uses a secret key for selecting the coefficients, it is not possible for unauthorized users to alter or remove the watermark.PSO based authentication system denotes effective authentication. From the experimental results, it is evident that the proposed encryption scheme offers very low encryption PSNR's and IQIM's is resistant to statistical analysis. This scheme attains the benefits of partial encryption as well as all the individual permutation techniques. The proposed encryption technique can be used applicable to protect against trespasser. The elevation of security can be further improved if necessary, by growing the size of the secret key and by growing the number of permutation in each round.

References:

Arne Jense and Anders la Cour-Harbo; Ripples in Mathematics: the Discrete Wavelet Transform by Springer, 2001.

Ashwin Swaminathan, Yinian and Min Wu, "Robust and secure image hashing", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, pp. 215-229, 2006.

Bruce Schneier, "Applied Cryptography", John Wiley and Sons, 1996.

Chai Wah Wu, "On the design of content-based multimedia authentication systems", IEEE Transactions on Multimedia, Vol. 4, No. 3, pp. 385-393, 2002.

Chih-Ming Kung ,Shu-Tsung Chao, Yen-Chen Tu ,Yu-Hua Yan, Chih-Hsien Kung , “A Robust Watermarking and Image Authentication Scheme used for Digital Contant Application”, Journal Of Multimedia, Vol. 4, No. 3, pp 112-119, June 2009.

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

Dittmann.J, S. Katzenbeisser, and A. Uhl , “Selective Image Encryption Using JBIG” , LNCS 3677, pp. 98–107, 2005.

Latha Parameswaran and K. Anbumani Content-Based Watermarking for Image Authentication Using Independent Component Analysis ,Informatica 32, pp 299-306, 2008.

Farhad Rahimi and Hossein Rabbani , “A dual adaptive watermarking scheme in contourlet domain for DICOM images”, BioMedical Engineering,vol 10, no 53,pp 1-18,2011.

Federica Battisti, Michela Cancellaro, Giulia Boato, Marco Carli, and Alessandro Neri , “Joint Watermarking and Encryption of Color Images in the Fibonacci-Haar Domain”, EURASIP Journal on Advances in Signal Processing , pp 1-13,2009.

Jinrong Zhu,” A Modified Particle Swarm Optimization Algorithm” Journal Of Computers, Vol. 4, No. 12, pp 1231-1236, December 2009.

Kennedy.J., R. Eberhart, "Particle swarm optimization", in Proceedings of the IEEE International Conference on Neural Networks (Perth, Australia), IEEE Service Center, Piscataway, NJ, pp.1942-1948, 1995.

Kuppusamy, K. Thamodaran , “Optimized Partial Image Encryption Scheme using PSO”, International Conference On Pattern Recognition, Informatics and Medical Engineering , March 2012, IEEE Explorer, 2012, pp 236-241.

K.Kuppusamy, K. Thamodaran , “Optimized Image Watermarking Scheme based on PSO”, International Conference On Modeling Optimization and Computing , April 2012, Elsevier Procedia Engineering 2012,vol 38, pp 493 – 503.

Maurice Clerc, Particle Swarm Optimization,ISTE publishers,First South Asian Edition,2007.

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

Muhammad Ishtiaq, Bushra Sikandar, M. Arfan Jaffar And Aziz Khan,”Adaptive Watermark Strength Selection Using Particle Swarm Optimization”, ICIC Express Letters,Volume 4, Number 5,pp 1-6, October 2010.

Panduranga H.T,Naveen Kumar S.K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images" , International Journal on Computer Science and Engineering, Vol. 02, No. 02, pp297-300, 2010.

Parthiban V, Ganesan R, "Hybrid Watermarking Scheme for Digital Images", Journal of Computer Applications, Volume-5, Issue EICA 2012-1,pp 85-95, 2012.

Rakesh S, Ajitkumar A Kaller, Shakshari B C and Annappa B, "A Novel Algorithm for Watermarking and Image Encryption", Computer Science & Information Technology, vol. 4, pp 347–356, 2012.

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

Xiaoyi Zhou, Jixin Ma, Wencai Du, Yongzhe Zhao, " Ergodic Matrix and Hybrid-key Based Image Cryptosystem", I.J. Image, Graphics and Signal Processing, vol 4, pp 1-9, 2011.

Zhou Wang, Alan. C. Bovik, "A universal image quality index", *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81-84, March, 2002.