International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Secure Optical Scanning Cryptography based Stereo Image Watermarking using Genetic Algorithm

Anshul Kanchan Khanna[A*] and Bhupendra Verma[B]

[A]Galgotias University, Greater Noida, India
[B]T.I.T. Excellence, Bhopal, India

Accepted 16 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

Watermarking has become an important tool for multimedia object creator or distributor to address the growing concern of multimedia owners. An attempt has been made to develop a complete secure digital stereo image non-blind watermarking system for effective copyright protection. The objective is to embed by watermarking into one stereo image the information needed to recover the other stereo pair (disparity image). A pre-processing stage has been added to the system to make it more robust and to enhance the security of the host image against intruders. The pre-processing stage includes encrypting the embedding medium by a digital simulation of the double random phase encoding based optical scanning cryptography. This encryption technique changes the gray-levels of pixels and hence is more secure than location scrambling algorithms that only change the positions of pixels and not the gray levels. The encryption technique used has also been proved to be secure against statistical, brute-force and key sensibility attacks. Further Genetic Algorithm has been employed for finding optimal values of embedding strength of watermarks. Genetic Algorithm thus frees the user from manually selecting embedding strength of watermarks which is a difficult task. The superiority of the proposed digital stereo image watermarking scheme has been shown by the excellent results achieved for peak signal to noise ratio and normalized correlation.

Keywords*: Digital Watermarking, Double Random Phase Encoding, DWT, Genetic Algorithm, Optical Scanning Cryptography, Stereo Image, Singular Value Decomposition*

1. Introduction

The tremendous growth of low cost internet and World Wide Web brought about a host of advantages with it. Multimedia data like images, audio and video could be inexpensively distributed or transmitted from one place to another with a single click. However these advantages were brought at the price of multimedia data being easily duplicated and distributed without the consent of the owner. The ease by which digital information could be duplicated and distributed led to the need for effective copyright protection tools. Thus various techniques have been developed and are still in progress to address the concern of the multimedia owner. It is done by hiding data (information) [Anderson, *et al*, 1998],[Cheddad, *et al*, 2010],[Bender, *et al*, 1996] within digital audio, images and video files. One way such data is hidden is in the form of digital signature, copyright label or digital watermark which completely characterizes the person who applies it and, therefore, marks it as being his/her intellectual property. Digital Watermarking is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object [Mohanty, 1999].

*Corresponding author **Anshul Kanchan Khanna** is working as Asst Prof and **Dr Bhupendra Verma** as Director

Computer science, cryptography and cryptographic protocols, digital signal processing and information and communication theory have all contributed to the success of digital watermarking technology [Chandramouli, *et al*, 2002] after its evolution from steganography. Watermarking may also use secret keys for copyright protection. In most watermarking applications additional information is also embedded. This information includes identifiers of the owner, recipient and/or distributor, transaction dates, serial numbers, etc. which play a crucial role in adding value to watermarking products[Kutter, *et al*, 1999],[Gonzalez, *et al*,1999].

Remaining part of the paper is organised as follows: section 2 discusses the related works in the field of watermarking. Section 3 explains the proposed watermarking scheme. Experimental results have been shown in section 4. Security analysis of the proposed encryption scheme is done in section 5. Section 6 is an analysis of the results. Finally, the paper is concluded with remarks and future work that can be carried out in this direction.

2 Related Works

The first digital watermarking proposals were made around the late 1970's and the early 1980's [Cox, *et al*,

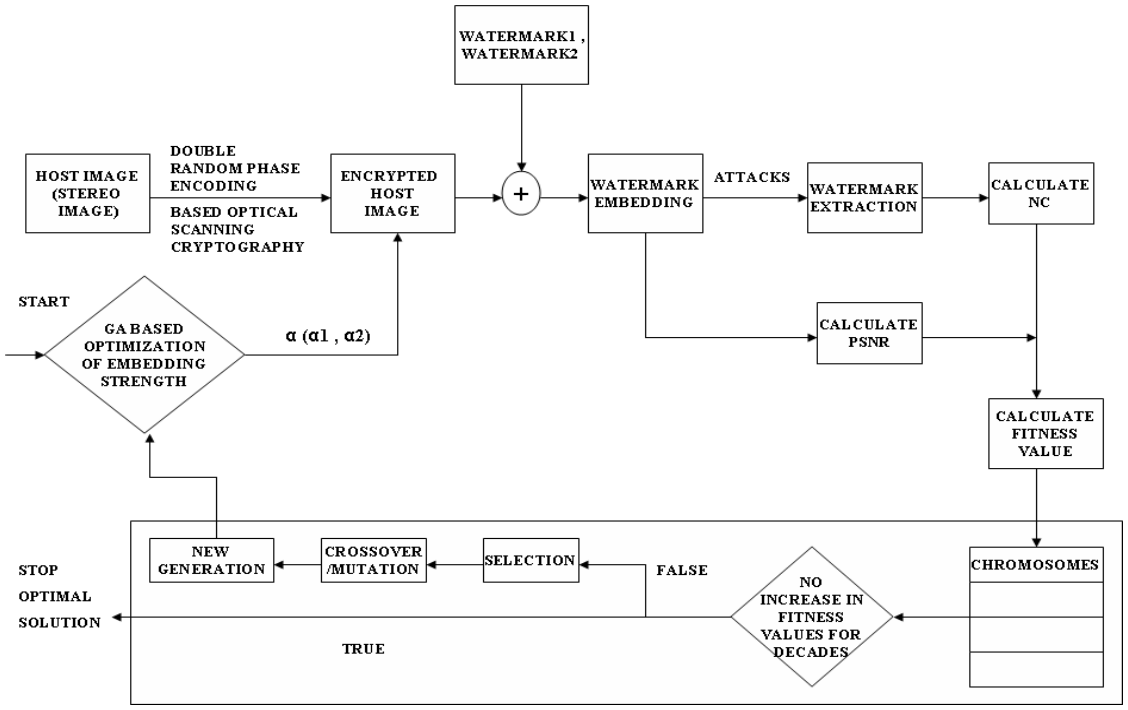


Fig 1 Proposed Model for Secure Digital Stereo Image Watermarking

2002]. The interest in digital watermarking began to mushroom since 1995 and since then many watermarking schemes have been proposed till date. Watermarking schemes have been proposed both in spatial domain and in the frequency domain. Spatial domain techniques include LSB substitution [Cox, *et al*, 2002], correlation based techniques[Bender, *et al*, 1995], patchwork based techniques[Bender, *et al*, 1995] and CDMA based techniques[Johnson, *et al*, 1995]. Frequency domain techniques modify the transform domain coefficients like DCT[Cox, *et al*, 1997], DFT[Runaidh, 1996] and DWT[Dugad, *et al*, 1998],[Kundur, *et al* , 1998] and are more robust than spatial domain techniques. One of the most cited frequency domain watermarking scheme was proposed by Cox *et al*[Cox, *et al*, 1997]. The performance of watermarking algorithms have been increased by employing various computational intelligence techniques[Darwish, *et al* , 2008] like neural networks [Zhang, *et al*, 2004], fuzzy logic[Chang, *et al*, 2005], swarm intelligence (ant colony optimization[Olariu, *et al*, 2006] and particle swarm optimization[Kennedy, *et al*, 1995]) , genetic algorithms[Shieh, *et al*, 2004],[Kumsawat, *et al*, 2004],[Aslantas,2007],[Huang, *et al*, 2008],[Boato, *et al*, 2008] or a combination of these. However a major problem still faced by digital watermarking systems is the security of multimedia data from unauthorized users or intruders apart from maintaining the robustness of the system. Although research has been done in this area by scrambling the host image using Arnold transform , magic square, zig-zag scanning, Hilbert transform, etc before embedding watermark to make the watermarking system secure against intruders but still an acceptable solution has to be worked upon as the above techniques used for scrambling only change the positions of pixels but do not change the gray levels of pixels. A technique that changes the gray levels of pixels can hide statistical information from intruders and can thus prove more beneficial than the commonly used location scrambling techniques.

3 Proposed Work

The idea proposed in section 2 has been taken into consideration when designing the stereo image watermarking system. To improve the security of host image, encryption of host image has been done by a digital simulation of double random phase encoding (DRPE) based optical scanning cryptography (OSC) [Poon, *et al* , 2003]. This technique changes the gray levels of pixels and is thus statistically secure. A graphical representation of the proposed secure digital stereo image watermarking system has been shown in fig 1. Firstly the host image is encrypted using DRPE based OSC. This technique has been shown to be secure against statistical, brute force and key sensibility attacks. Watermarks are then embedded into the encrypted host image. The embedding strength of watermarks is calculated using a genetic algorithm approach. PSNR (Peak signal to noise ratio) and NC (Normalized correlation) values are calculated to compare the proposed watermarking scheme to the existing ones.

The whole process has been divided into the following phases:

3.1 Pre-Processing Stage (Encryption of host image)

Our main consideration when designing the algorithm was the security of the stereo image apart from high robustness of the system. To make the digital watermarking system secure, a pre processing stage has been proposed which includes encryption of the host

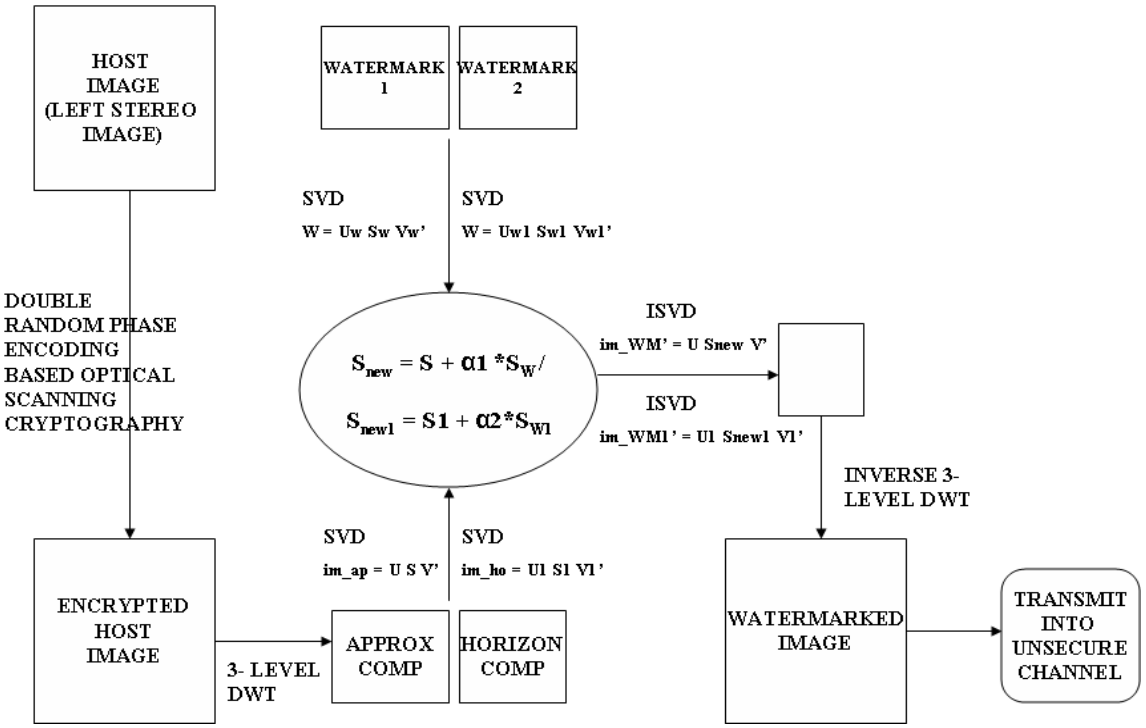


Fig 2 Watermark Embedding

image. The host image is the left stereo image of the stereo pair. A digital simulation of the optical scanning cryptography combined with the famous double random phase encoding technique[Poon, *et al*, 2003] has been used to encrypt the image. This technique is more secure than either double random phase encoding [Refregier, *et al*, 1995],[Unnikrishnan, *et al*, 2000], [Nishchal, *et al*, 2008], [Situ G, *et al*, 2006], [Towghi, *et al*, 1999] or optical scanning cryptography[Poon , 2007],[Javidi, 2005]. Besides a digital simulation of it makes us rid of the physical setup, unavailability of hardware or low cost optoelectronics and gives us more flexibility as we can virtually select a wavelength instead of a physical laser light source[Peng, *et al*, 2002]. The encryption is done as follows:

Encrypted image = $\mathcal{F}^{-1}$ { $\mathcal{F}$ { Original Image * First Random Phase mask} * OTF * Second Random Phase Mask} (1)

Where OTF is the optical transfer function of the system[Poon, 2007]. The two random functions are chosen independently of each other and are of the same size as host image and having values between 0 and 1 and symbol $\mathcal{F}$ represents fourier transform [Poon , *et al*, 2003].

The above encrypted image can be decrypted when required by taking inverse of encryption as given below:

Decrypted image = $\mathcal{F}^{-1}$ { $\mathcal{F}$ { Encrypted Image}* conjugate(OTF * Second RPM) } (2)

Thus the intensity (absolute value) of the decrypted image gives the original image.
This pre-processing stage which includes encrypting of host image has been done for two reasons:

- It gives better security of watermarking scheme by setting encryption keys. Thus only the authorized users know the secret keys to decrypt the original host image which is thus protected against intruders.
- It makes the watermark bits spread uniformly over the host image . Thus it can resist attacks like cropping, filtering and compression effectively.

3.2 Watermark Calculation

Watermarking has been done on stereo images. The basic problem with stereo images is finding the co-ordinates of the pixel on the left and right images which correspond to the same world point and is known as stereo correspondence problem[H S Singh, *et al*, 2011],[Scharstein D, *et al*, 2002],[Brown, *et al*, 2003]. Since stereo pair represents two images of the same world scene that differ slightly from each other. So the storage and transmission of a stereo pair requires twice the space and bandwidth as needed for a single image[T Frajka, 2003],[D Coltuc, 2007]. To eliminate this problem and treat stereo pair as a monocular image, a disparity image has been estimated from the stereo pair which serves as our watermark. The disparity image is basically the difference image of the two stereo pairs. The disparity image estimated from the stereo pair serves as our watermark. Any change in watermark will ultimately mean a change in either the left stereo image or a change in right stereo image or both. The watermark is calculated as follows:

(a) The approximation sub band of DWT represents approximately the same image. A third level DWT decomposition of the stereo pair is done to reduce computation cost by 64.

(b) The approximate image pairs(AI_L and AI_R) are further used to calculate disparity between them by[H S Singh, *et al*, 2011]:
   (i) Matching cost computation using sum of squared differences of intensity values.
   (ii) Cost (support) aggregation.
   (iii) Disparity computation using winner takes all strategy(WTA).

Thus the above watermark halves the storage and bandwidth requirements and can be used to correctly retrieve the right stereo pair. However the above watermark cannot prove ownership in case of disputes as it contains no identity of the owner, so considering this fact a second watermark has been embedded in the host image. This watermark can establish copyright protection in case of multiple ownership claims. Our second watermark is simply a logo with words WM on it. These two watermarks are embedded in different subbands[E Ganic, *et al* , 2004].

3.3 Watermark Embedding

The following approach has been used for watermark embedding:

- Encrypt the host image (left stereo image) (im_L) by double random phase encoding based optical scanning cryptography. Let encrypted image be im_L' .
  - Perform 3-level DWT decomposition on encrypted image. Let its approximation component of 3-level be im_ap and horizontal component be im_ho.
  - Perform SVD on im_ap and im_ho i.e. im_ap = U S V' im_ho= U1 S1 V1'
  - Perform SVD on both the watermarks (calculated in 3.2) W and W1
    W = Uw Sw Vw'
    W1 = Uw1 Sw1 Vw1'
  - Modify the singular values of encrypted host image with the singular values of the watermark as follows :Snew = S + α1x Sw
    Snew1 = S1 + α2 x Sw1
    where α1 is the embedding strength of first watermark and α2 is the embedding strength of second watermark and are calculated using genetic algorithm.
  - Perform inverse SVD i.e.
    im_WM' = U Snew V'
    im_WM1' = U1 Snew1 V1'
  - Perform inverse 3-level DWT to obtain watermarked encrypted image im_WM.

This encrypted watermarked image is then transmitted in the insecure channel.

3.4 Watermark Extraction

The watermarks are extracted with the help of following algorithm. Let the received watermarked encrypted image be im_WM_R after applying attacks . Since this is a non-blind watermarking scheme the original host image is required for extraction. The encrypted original image is im_L' .

- Perform 3-level DWT on received watermarked encrypted image im_WM_R to get $im\_WM_{R'}$ Let its approximation component be im_app and horizontal component be im_hd .
- Perform SVD on im_app and im_hd
  im_app = $U_{new'}$ $S_{new'}$ $V_{new'}$'
  im_hd = $U_{new1'}$ $S_{new1'}$ $V_{new1'}$'
- Perform 3-level DWT on encrypted host image im_L' to get its approximation component im_ap1 and horizontal component im_hd1.
- Perform SVD on im_ap1 and im_hd1
  im_ap = U S V'
  im_ho = U1 S1 V1'
- Find the singular values of the extracted watermarks as follows:
  $S_{W'} = (S_{new'} - S)/ \alpha 1$
  $S_{W1'} = (S_{new1'} - S1)/ \alpha 2$
- Perform inverse SVD to get the extracted watermarks i.e.
  W1' = Uw1 Sw1 Vw1'

3.5 Binary Coded Genetic Algorithm

Since it is very difficult to manually set a value for embedding strength of watermarks which gives maximum imperceptibility and maximum robustness, so Genetic Algorithm[Holland, 1992],[Goldberg , 1989] has been employed to find an optimal value for embedding strength that maximizes both the requirements and frees the user from this difficult task. In our proposed algorithm a binary coded genetic algorithm has been used for optimization.

The following parameters have been set for GA:
Initial Population : 20
Length of chromosome : 18
Crossover Probability : 0.95
Mutation Probability : 0.05
Number of generations : 60
Fitness Function (f) = $PSNR(\alpha 1, \alpha 2) + 1/n \Sigma i=1\ n\ W * NC1i\ (\alpha 1) + 1/n \Sigma i=1\ n\ W * NC2i\ (\alpha 2)$

where W is a weighting factor for the Normalized Correlation values. The value of W has been fixed to be 550 in our experiments. NC1 is the normalized correlation between original watermark1 and extracted watermark1 while NC2 is the normalized correlation between original watermark2 and extracted watermark2 and n represents the total number of attacks that we have considered. Value of n is 4 as we have taken 4 types of attacks in consideration. Because the PSNR values are dozens
of times larger than the NC values , so the NC values are magnified by weighting factor W to balance the imperceptibility and robustness requirements.

Crossover: A 2- point crossover operator has been applied in the proposed algorithm. For crossover firstly the two parents have been selected by roulette wheel selection method from the whole population and then the genetic operators have been applied. With fitness proportionate selection there is a chance that some weaker solutions may survive the selection process. This is an advantage because

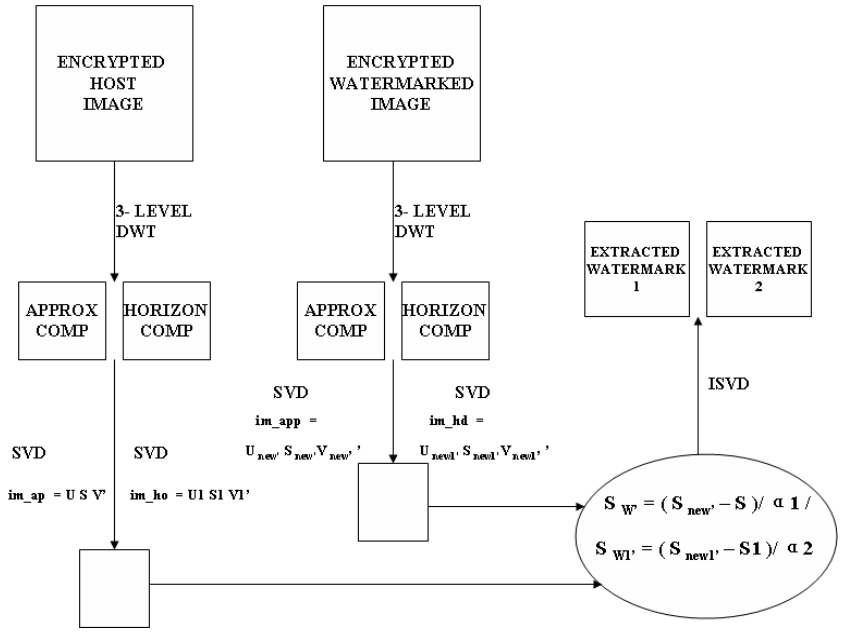


Fig 3 Watermark Extraction

Stereo Image Pair: Arch

Table 1 Comparative table for stereo image pair Arch

	Reference[Kumar, Balasubramanian, 2009]	**Reference**[Kumar, Raman, Thakur, 2009]	**Proposed Scheme (NC for watermark1, watermark2)**	
PSNR	41.3744	44.05	49.2514	
			Watermark1	**Watermark2**
NC(Average Filtering)	0.9757	0.88084	0.9898	0.9937
NC(Rotation)	0.9801	0.8987	0.9597	0.9558
NC(Resizing)	0.9672	0.9100	0.9946	0.9893
NC(Gaussian Noise)	0.9700	0.9042	0.9912	0.9503

Stereo Image Pair: Fruit

Table 2 Comparative table for stereo image pair Fruit

	Reference[Kumar, Balasubramanian, 2009]	**Reference**[Kumar, Raman, Thakur, 2009]	**Proposed Scheme (NC for watermark1, watermark2)**	
PSNR	40.5072	42.51	48.3991	
			Watermark1	**Watermark2**
NC(Average Filtering)	0.9803	0.9240	0.9877	0.9952
NC(Rotation)	0.9841	0.9308	0.9322	0.9674
NC(Resizing)	0.9730	0.9094	0.9936	0.9959
NC(Gaussian Noise)	0.9721	0.9027	0.9903	0.9406

Stereo Image Pair: Parts

Table 3 Comparative table for stereo image pair Parts

	Reference[Kumar, Raman, Thakur, 2009]	**Proposed Scheme (NC for watermark1, watermark2)**	
PSNR	42.97	48.3883	
		Watermark1	**Watermark2**
NC(Average Filtering)	0.9002	0.9894	0.9954
NC(Rotation)	0.9118	0.9207	0.9625
NC(Resizing)	0.8975	0.9943	0.9965
NC(Gaussian Noise)	0.8796	0.9878	0.9448

even a solution may be weak but it may include some component which may prove useful after the recombination process.

Mutation: A random mutation operator has been applied.

Selection: To repeat the process again for the next generation, a new population of chromosomes or individuals has to be created. This is done by selecting 4 individuals from previous population by truncation selection method. This ensures that good chromosomes from previous population are not lost and are carried to the next generation. The other 16 individuals are created by applying crossover and mutation on the previous generation to create new individuals. Thus the new population is a good blend of previous good chromosomes and new chromosomes.

4 Experimental Results

Experiments have been done on three stereo image pairs Arch, Fruit and Parts.

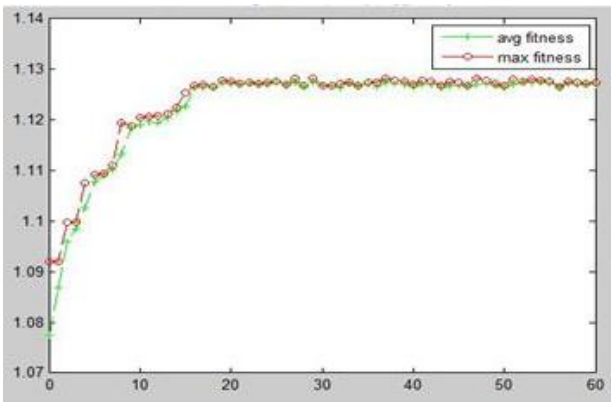


Fig 4 Fitness values against Generations for image Arch

These images have been downloaded from the Vision and Autonomous Systems Center's Image Database of Carnegie Mellon University [http://vasc.ri.cmu.edu/idb/html/stereo/index.htm]

All the stereo pairs are of size 512x512. The watermarks are of size 64x64.

Fig 4 shows a graph of the fitness values against generations for image Arch. The average and maximum of all the fitness values in a generation is calculated and plotted. A comparison has also been done of our proposed scheme with the results of references [Kumar, Raman, Thakur, 2009], [Kumar, Balasubramanian, 2009].

5 Security analysis of proposed encryption scheme

Tests have also been conducted to prove the security of our encryption algorithm against statistical attacks, brute force attack and key sensitivity[Loukhaoukha K, *et al*, 2012]. The results have been summarized below:

A Statistical Analysis

To prove the robustness of the proposed image encryption procedure, statistical analysis has been done by calculating the histograms and the correlation coefficient of adjacent pixels in the encrypted images.

(i) Histogram analysis

An image-histogram shows how pixels in an image are distributed by plotting the number of pixels at each intensity level. From the graphs below we see that the histogram of original image is significantly different from its encrypted version using the proposed algorithm. However for Arnold transform and zigzag scanning the histograms of original image and scrambled image are similar to each other which may thus provide statistical information to the intruders.

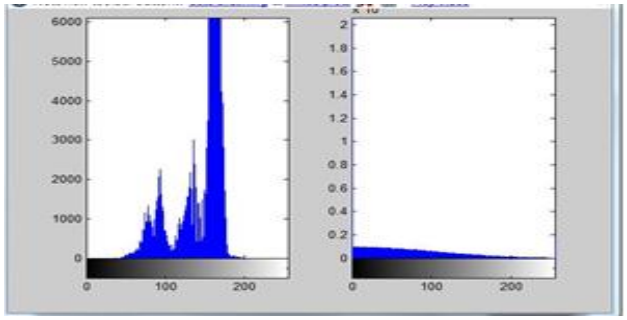


Fig 5. Histogram Analysis of Original image(Arch) and encrypted image (DRPE based OSC)

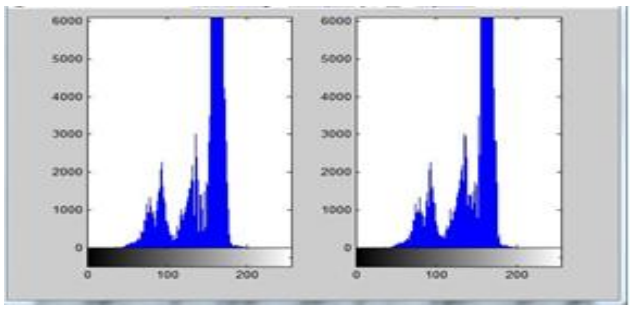


Fig 6 Histogram Analysis of original image (Arch) and encrypted image (Arnold transform)

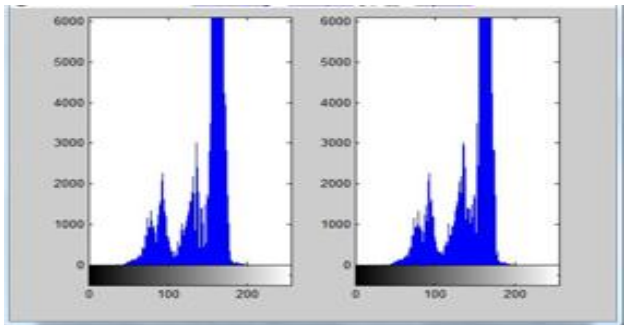
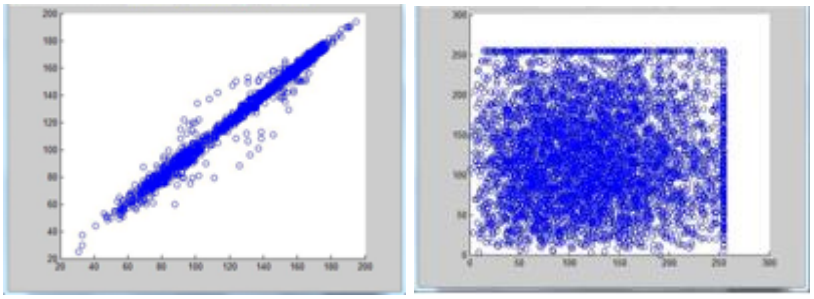


Fig 7 Histogram Analysis of original image (Arch) and encrypted image (Zigzag scanning)

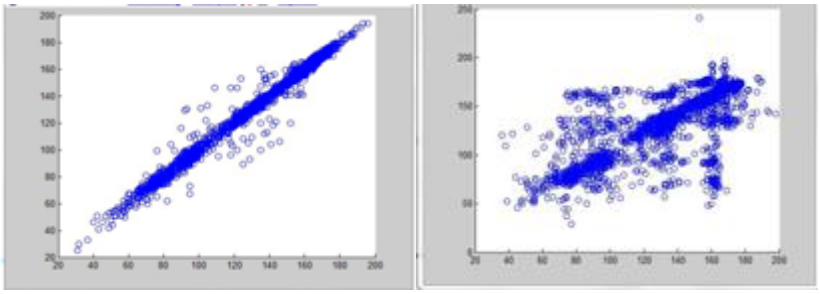
(ii) Correlation analysis

In general, there is strong correlation between two adjacent pixels in an image. Thus scrambling algorithms



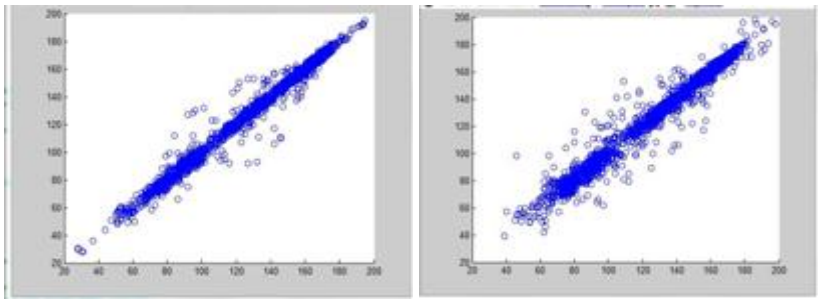
(a) **(b)**

Fig 8 Correlation Analysis using proposed encryption technique (a)Original Image (b) Encrypted Image



(a) **(b)**

Fig 9 Correlation Analysis using Arnold transform (a) Original Image (b) Encrypted Image



(a) **(b)**

Fig 10 Correlation Analysis using Zig-zag scanning (a) Original Image (b) Encrypted Image

should have strong de-correlation ability to destroy such correlation i.e. the correlation coefficient should be as less as possible. Correlation analysis has been done by calculating correlation in horizontal direction by selecting 5000 pairs randomly in that direction. The following results were obtained.

Table 4 Correlation coefficients of adjacent pixels

Correlation among adjacent pixels in horizontal direction	**Proposed Encryption Technique**	**Encryption using Arnold Transform**	**Encryption using Zigzag scanning**
Original Image (Arch)	0.9946	0.9943	0.9950
Encrypted Image	0.0136	0.8233	0.9903

Graphical representations of correlation among 5000 pairs of adjacent pixels in horizontal direction using proposed encryption technique, Arnold transform and Zig-Zag scanning are shown below.

B Key Space Analysis

A secure image encryption algorithm must have a large key space to make the brute force attack computationally infeasible. An amplitude based double random phase encoding(DRPE) technique has a large key space. A system with a phase key that has NxM pixels each with Q quantization levels has $Q^{(2xNxM)}$ keys, if perfect decryption is applied.

However after applying the reduced brute-force attack, the number of keys is reduced to $Q^{(NxM)}$ .Thus our technique having 512x512 pixels and 512 quantization levels has a very large key space. Thus the key space of amplitude based double random phase encoding is $512^{(512x512)}$ [Y Frauel, *et al*, 2005].

On further applying the approximations the key space can be reduced to $2^{(512x512)}$ for imperfect decryption using 2 quantization levels. Besides the extra parameters z^c and virtual wavelength in OTF in our algorithm further add to the security of the algorithm. Thus due to the large key space , brute force attack is computationally not feasible.

On the other hand, the key space of Arnold transform is too small and so it is susceptible to brute force attack. Also the security of zigzag scanning depends only on the secrecy of algorithm as it has no additional parameters.

C Key Sensibility Analysis

An Encryption algorithm should have high sensibility to the encryption key. This means that any small change in the key should lead to a significant change in the encrypted, or decrypted, image. An ideal image encryption algorithm should be sensitive with the secret key. Tests were conducted to prove this by changing the keys for decryption. It was observed that the decryption with a slightly different key fails completely. The results obtained are shown in figure below:

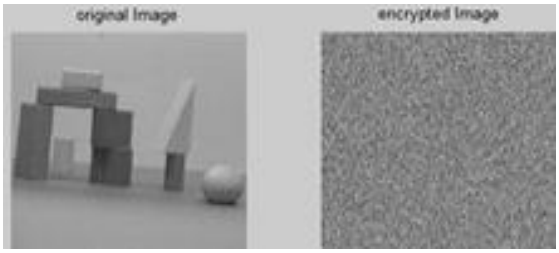


Fig 11 Original image and encrypted image

6 Result Analyses

From the experimental results depicted in above tables, it can be seen that if encryption is done using double random phase encoding based optical scanning cryptography then robustness can be increased. The security of the host image from unauthorized users also increases. The location scrambling techniques like Arnold transform , magic square transform, zigzag scanning , etc change the positions of pixel values. The grayscale of each pixel still remains its original value which is insecure[Z Tang, 2011],[Z Shang, *et al*, 2008],[Ruisong Ye, 2009],[Z Yanqun, *et al*, 2009]. Also the security of encrypted image using proposed encryption technique is not solely dependent on the secrecy of algorithm. Even if the intruders come to know about the algorithm used, still the key space is too large to conduct an exhaustive search. On the other hand transforms like zig-zag, Arnold can be easily reversed. The proposed encryption technique also does not require any pre-processing such as that needed in Arnold transform (for conversion to square images) [L P Shao, *et al*, 2008]. Our proposed digital watermarking system is far better secure than the existing ones. Further Genetic algorithm have shown their superiority in finding optimal values of embedding strength of both the watermarks.

Conclusion

Digital Stereo Image Watermarking is a difficult problem and considerable less amount of research has been done in the field of watermarking stereo images. This paper was an attempt to develop a secure digital stereo image watermarking system for effective copyright protection. Various problems of digital watermarking systems like security, susceptibility to attacks and the imbalance between the major requirements of watermarking have been sorted out by the proposed digital watermarking model. The results obtained here support the use of double random phase encoding based optical scanning cryptography for encryption of host image in digital watermarking systems and the use of Genetic Algorithm for optimizing results. Further the watermark can also be encrypted using the proposed encryption technique before embedding so as to make the system more secure. Also the concept of multiple scaling factors can be applied to our system to make it more robust. GA can used to optimally determine the scaling factors for watermarking process.

References

R J Anderson, F A P Petitcolas, (1998) On the limits of steganography Special issue on copyright protection and privacy protection, IEEE Journal on selected areas in communication, ISSN 0733-8716, vol 16 issue 4 pp 474-481.

A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, (2010) Digital image steganography : survey and analysis of current methods, Elsevier Signal processing vol 90, issue 3 pp 727-752.

Bender W., Gruhl D., Morimoto N, Lu A., (1996) Techniques for data hiding, IBM Systems Journal, vol 35, No. 3 ,4 pp. 313-335.

Saraju P. Mohanty, (1999) :Digital Watermarking : A tutorial review.

R Chandramouli, Nasir Memon, Majid Rabbani, (2002) Digital watermarking, Wiley.

M. Kutter, F. Hartung, (1999) Introduction to watermarking techniques, in Information techniques for steganography and digital watermarking, pp. 97-119.

F. P. Gonzalez, J. R. Hernandez, (1999) A tutorial on digital watermarking.

I.J. Cox, M.L. Miller & J.A. Bloom, (2002) Digital watermarking Morgan Kaufman publishers, Academic Press, USA, 542 p. ISBN 1-55860-714-5.

Bender W., Gruhl D., Morimoto N., (1995) Techniques for data hiding, Proc. SPIE, Storage and Retrieval for Image and Video Databases III, vol. 2420, San Jose, CA, pp. 165-173.

Bender W., Gruhl D., Morimoto N., (1995) Techniques for data hiding, Proc. SPIE, vol. 2420, pp 40.

I.J. Cox, J.Killian, F.T. Leighton, T. Shamoon , (1997) Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687.

J.J.K. O. Runaidh , (1996) Phase Watermarking on Digital Images, Proc. IEEE, International Conf. On Image Processing, ICIP, vol3, pp 239-242.

R. Dugad, K. Ratakonda, and N. Ahuja, (1998) A new wavelet-base for watermarking image, in Proc. Int. Conf. Image Processing, Vol. 2, pp. 419–423.

S. Kumar, B. Raman, M. Thakur, (2009) Real Coded Genetic Algorithm based Stereo Image Watermarking, International Journal of Secure Digital Information Age, vol 1, no 1.

D. Kundur and D. Hatzinakos, (1998) Digital watermarking using multi-resolution wavelet decomposition, in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Vol. 5, Seattle, WA, pp. 2969–2972 .

A. Darwish, A. Abraham, (2008) The use of computational intelligence in digital watermarking: review, challenges, and new trends, International Journal on non-standard computing and artificial intelligence, vol 21, pp 277-297.

N.F. Johnson, S.C. Katezenbeisser, (1999) A survey of steganographic techniques in Information techniques for steganography and digital watermarking, pp. 43-75.

Fan Zhang, Hongbin Zhang, (2004) Applications of neural network to watermarking capacity, International symposium on communications and information technologies.

Chip-Hong Chang, Zhi Ye, Mingyan Zhang, (2005) Fuzzy-ART Based adaptive digital watermarking scheme, IEEE transactions on circuit and systems for video technology, vol.15, no.1.

S. Olariu, A.Y. Zomaya (Eds.), (2006) Handbook of bioinspired algorithms and applications, Chapman & Hall/CRC, ISBN-10: 1584884754.

J. Kennedy, R. Eberhart, (1995) Particle swarm optimization, Proceedings of IEEE international conference on neural networks, vol 4, pp. 1942-1948.

Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-Hsing Wang, Jeng-Shyang Pan , (2004) Genetic watermarking based on transform domain techniques Science Direct Pattern Recognition vol 37, pp 555-565.

P. Kumsawat, K. Attkitmongcol, A. Srikaew, S. Sujitjorn , (2004) Wavelet based image watermarking using genetic algorithm Springer-verlag Berlin Heidelberg, pp 643-649.

J.H. Holland, (1992) Adaptation in natural and artificial systems, The MIT press.

D.E. Goldberg, (1989) Genetic Algorithms in search, optimization, and machine learning, Addison-Wesley professional.

Tamas Frajka, Kenneth Zeger, (2003) Residual image coding for stereo image compression, Society of photo-optical instrumentation engineers.

P. Refregier, B. Javidi, (1995) Optical image encryption based on input plane and Fourier plane random encoding, Optical Letter 20 , pp 767-769.

H.S. Singh, Rachna, A. K. Verma, (2011) Efficient Window based Disparity Map calculation for stereo matching, Journal of Computer and Mathematical Sciences, vol 2 , issue 2, pp 182-189.

Ting-Chung Poon, Taegeun Kim, Kyu Doh, (2003) Optical scanning cryptography for secure wireless transmission, Optical Society of America, vol 42, no 32.

Ting-Chung Poon, Optical Scanning Holography with Matlab , Springer, 2007.

Bahram Javidi, (2005) Optical and Digital Techniques for Information Security, Springer.

Daniel Scharstein, Richard Szeliski, (2002) A taxonomy and evaluation of dense two-frame stereo correspondence algorithms, International journal of computer vision, vol 47 pp 7-42.

M. Z. Brown, D. Burschka, G D. Hager, (2003) Advances in computational stereo, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 25, no. 8.

Dinu Coltuc, (2007) On stereo embedding by reversible watermarking, IEEE.

G. Unnikrishnan, Joseph J, Singh K, (2000) Optical encryption by double random phase encoding in the fractional fourier domain, Opt. Lett 25 pp 887-9.

Nishchal N K, Joseph J, Singh K, (2008) Fully phase encryption using fractional fourier transform, Opt. Eng. 42 pp 1583.

Situ G, Zhang J, (2006) Double random phase encoding in the Fresnel domain, Opt. Lett. 29 1584.

N. Towghi, B. Javidi, Z. Luo, (1999) Fully phase encrypted image processor, Journal of Optical Society of America, vol 16 issue 8, pp 1915-1927.

Emir Ganic, Ahmet M. Eskicioglu, (2004) Robust DWT-SVD Domain Image Watermarking: Embedding data in all frequencies, ACM 1-58113 pp 854-857.

http://www.optiwater.com/optiga/ga.html

http://vasc.ri.cmu.edu/idb/html/stereo/index.html

S. Kumar, R. Balasubramanian, (2009) An optimally robust digital watermarking algorithm for stereo image coding, Springer Rec. Advances in multimedia signal process and comm. , SCI 231, pp 467-493.

K. Loukhaoukha, J.Y. Chouinard, A. Berdai, (2012) A secure image encryption algorithm based on Rubik's cube principle, Journal of electrical and computer engineering, vol 2012, no 7, article id 173931.

Zhenjun Tang, Xianquan Zhang, (2011) Secure image encryption without size limitations using Arnold transform and random strategies, Academy Publisher, jmm.6.2 pp 202-206.

Zhenwei Shang, Honge Ren, Jian Zhang, (2008) A block location scrambling algorithm of digital image based on Arnold transformation, IEEE 9th International conference for young computer scientists.

Ruisong Ye, (2009) A novel image scrambling and watermarking scheme based on orbits of Arnold transform, IEEE Pacific – Asia Conference on Circuits, Communications and System.

Zhang Yanqun, Wang Qianping, (2009) A new scrambling method based on Arnold and fermat number transformation, IEEE International conference on environmental science and information application technology, 978-0-7695-3682-8.

Veysel Aslantas (2007) An SVD based digital image watermarking using genetic algorithm , IEEE.

Hsiang-Cheh Huang , Chi-Ming Chu, Jeng-Shyang Pan , (2008) The optimized copyright protection system with genetic watermarking Springer-Verlag.

G. Boato, V. Conotter, F G B De Natale, (2008) GA based robustness evaluation method for digital image watermarking Springer-Verlag, pp. 294-307.

L.P. Shao, Z. Qin, H.J. Gao, X.C. Heng, (2008) 2D Triangular Mappings and their applications in scrambling rectangle image, Information Technology journal, vol 7, pp 40-47.

Y.Frauel, A.Castro, T.J.Naughton, B.Javidi, (2005) Security analysis of optical encryption, Proc. Of SPIE, Unattended sensors and sensor networks II, vol. 5986.

X Peng, L Yu, L Cai, (2002) Double-lock for image encryption with virtual optical wavelength, Optics Express 41, vol 10, no 1, Optical Society of America.